第三版序

现在呈现在读者面前的是本书的第三版．这本书曾在四分之一世纪里在力所能及的范围内对群论的发展起了促进的作用．作者在1940年完成了这本书第一版的工作，第二年进行了两次校对．只是由于战时的情况，本书被推迟到1944年才得以问世．在第一版的序言里——这个序言的大部分都摘录在后面——指出了作者在本书中所致力的目标．

在四十年代，一般群论得到蓬勃的发展．在阿贝尔群的理论方面，在直积的理论方面，在可解群、幂零群和具各种有限性条件的群的理论方面，都取得了显著成就．由 О. Ю. Шмидт 所创立的苏联群论学派在这个发展中起了很大的作用．特别，按照本书第一版学习群论的苏联年轻的代数学家做了许多工作 —— 应该提一下，本书在1940年的打字原稿保存在莫斯科大学数学力学系，也为研究带来了方便．

书的第二版完成于1952年，而是在1953年出版的．这本书反映了五十年代初期群论所达到的状态．从题材的重新安排来看，从很多新的章节的增加来看以及从对于第一版的许多内容的充分修改来看，这本书实际上已是一本新书．只是由于新书是以旧书为基础，并且在构思上与旧书非常接近，才使作者保留了旧的书名．

在此期间，世界各国相继出版了本书的译本．1953年德意志民主共和国出版了第一版的德文译本．晚后出版了第二版的一些译本：1955年出版了匈牙利文译本；1955和1956年先后出版了英(美)文的两卷译本；1959年出版了罗马尼亚文译本；1960和1961

年先后出版了日文的两卷译本;中文译本(第一卷)则在1964年出版的. 这样就使本书得以参与世界上许多国家的群论发展.

五十年代和六十年代前五年是群论取得进一步发展的时期. 多年来,甚至几十年来有待解决的问题被解决了. 比如我们将提到的关于周期群的Burnside问题以及关于具有限个定义关系的群的算法问题. 阿贝尔群的理论经受了根本的改造. 在可解群和幂零群的理论方面也做出了很多成果. 整个新的方向形成了——比如说,群流形的理论,群类(即抽象群的性质)的理论,群上运算的理论,自同构群和群偶的理论. 在群论基础方面也发生了重要的变化. 例如,从算子群过渡到多重算子群.

在这一时期,关于一般群论研究的兴旺程度单从研究著作的数量上就足以说明. 在本书第二版里所载入的十分完全的文献大约有五百篇. 另一方面,在完成第二版以后的若干年里,关于一般无限群论方面的论文(即不包括有限群,置换群,线性群,Lie群和代数群,拓扑群,有序群以及模论等方面的工作)不下1300篇(其中苏联作者的工作约占三分之一).

近年来,发表了一般群论的某些分支的专门论著. 这样的专门论著今后还将会继续出现,这是理所当然的. 然而,不言而喻,与此同时全面地阐述群的理论,并且将它作为统一的学科而保存着的综合文集也是必要的. 这些年来,一些带有一般性特征的书在各个国家出现了. 每一本书都有它自己的长处,但遗憾的是,这些书的任何一本都未能充分满足所指出的要求. 这就是出版本书新版的原因.

作者很清楚,实际上应该写一部新的书. 但是作者知道,在上述如此丰富的材料的情况下,这本书就应该是三卷集,而作者已经不可能计划如此浩繁的工作了. 因此,这个第三版就有着非常不一般的形式.

这就是，在第三版中，以不多的变化保留了第二版的全文，改正了某些不正确的地方和一些印刷上的错误，以及一些不太现代化的符号. 重印旧书的全文是有道理的，因为旧书早已绝版，甚至一些年轻的苏联群论工作者的家中也没有这部书.

印刷数量相当少的第一版就更是珍本了. 然而，正象作者在第二版序言里所说的那样:“由于不可避免的篇幅的扩大，作者不得不将旧书的许多地方完全删去，有时甚至是整节地删去，而这些内容过去写入书中并不能认为是错误的.”所以第二版的读者不止一次地要参看第一版的有关段落；并且到目前其他一些作者还不得不援引本书的第一版.

由于这个原因，在第三版里，有些第二版的原文也包含了第一版的某些材料. 有时是整节地引入；同时对这些节这样编号，就是在原第二版的节的号码后面缀上字母 a(有时还要缀上 б 和 в). 这样读者就可以不费力地按目录找到这些节. 第一版中的某些材料还收集于 §§ 23,26,33,35,42,44,53,54 中.

现在这本书的基本正文就是这样. 本书也载入了《第一版的结束语》. 显然，过了四分之一世纪，作为描绘群论进一步发展道路的纲要，它的作用已经完全消失，其中很多地方现在看起来甚至很幼稚. 然而，把当时还年轻的作者在那时候所提供的大纲与科学的实际发展作一比较，可能是有益的. 我们对《结束语》的原文没有作任何修改；只是在引用第一版的章节时把它换成这本书基本正文相应节的号码(圆括号). 此外，在方括号里指出基本正文或者其后面的《补充》的各节的号码. 在补充里读者可以找到所考虑的问题进一步发展的信息.

带有标题为《1952—1965 年无限群论的发展》的补充对于专家可以说是最有用的. 在补充里，作者试图对第二版完成以后的年代里一般群论的发展作一概述. 同时也说到一些更早的工作.

如果说这些工作在第二版中没有得到充分反映的话，作者也认为是不合适的．另一方面，作者显然不可能在概述中以应有的完备性反映关于近年来的文献；不过这方面已为刊载在《科学成果》丛刊里的摘要所弥补．

《补充》的结构没有重复基本正文的结构，并且可以这样说，如果作者现在写这本书的话，关于群论新书的结构应该是这个样子．《补充》不包含任何论证；然而，所有必要的定义都已被引入，并且将某些结果表述出来．在《补充》中总共提到一千一百篇论文，这些论文没有列入第二版的文献索引．然而，其中的一些只是被提到一下．只是把所有这些工作补充收进文献索引里．和通常一样，引用这个索引时，指出作者的姓名和被引用的文献的编号(在方括号内)．

在基本正文里多次建议参看《补充》．[参看补充 12.3] 意味着“参看补充 § 12，第三段”．

在《补充》的正文里，如果不是说它的前言的话，几乎没有涉及有限群论的成果．作者在本书第二版序里曾经说过：“在进行第一版的工作时，作者面临的任务是要指出群论不只是有限群论，因而这本书几乎不包含任何关于有限群的特别论述．现在这个任务可以认为已经完成．相反地，提出了新的问题——要注意有限群论是一般群论的一个重要组成部分．尽管已在书中补充了一些与有限群有关的题材，但是这个新的任务在本书中还没有完全解决．”关于有限群论各方面问题所发表的著作的数量是如此巨大，以致作者在写第三版《补充》时也无法试图解决这个问题，虽然作者明白，如果以前脱离出去的分支再重新成为统一理论的有机组成部分，那末群论被分成各个独立分支的倾向就会逐渐受到制止．

近年来在群论中做了大量的工作．群论的研究正在非常紧张地进行．看来，作者现在难以再重复他在第一版序言中曾说过的

这样一句话，即："一般群论还没有达到它本身发展的顶峰."然而，群论对于更一般的代数的理论，比方说，泛代数的理论和范畴的理论，无疑仍将继续是新思想的基本提供者和试验场所. 可以期望，最近一些年里群的理论工作者的研究仍会保持着非常强烈的势头. 如果这本书在它的新版里还能在一段时间内对从事群论的代数工作者有所裨益，作者将感到高兴.

作者谨向在这本书的第三版的工作中所有给予他帮助和支持的人致以诚挚的谢意，首先是 А. П. Мишина, А. Л. Шмелкин 和 Е. Г. Шульгейфер. 特别要感谢承担繁重的编辑任务的 О. Н. Головин，作者对于他重新作为自己的合作者而感到愉快——顺便提一下，Олег Николаевич 曾经是本书第一版的编辑之一.

А. Курош

1966 年 11 月于莫斯科

第一版序摘要

群论有着悠久和丰富的历史. 它是随同 Galois 理论一起，为了这一理论的需要而产生的，并且首先是作为有限置换群的理论而发展起来的(Cauchy, Jordan, Sylow). 然而，不久就发现，对于有关这一理论的大多数问题来说，用以构成群的特殊材料——置换——并不重要，而实际所应注意的只是对于在任意有限集合里所定义的代数运算的性质的研究. 这样一个现在看起来是不言而喻的发现，实际上是一个很大的成就，并且使得有限群的一般理论得以形成. 不错，由置换群过渡到一般有限群论实质上并没有丰富了研究对象，但是这样的过渡就把群论建立在公理基础上，使它变得严谨而清晰，从而有利于这一理论的进一步发展.

上世纪末和本世纪的最初十年里是有限群论的全盛时代. 在这期间，有限群的主要结果被得到了，主要研究方向被指明了，主要研究方法被建立了；一般说来，有限群论通过这方面主要学者(Frobenius, Hölder, Burnside, Schur, Miller)的工作，在当时已经具备了它在今天[1]所带有的一切主要特征. 然而以后逐渐显示出来，群的有限性是一个过于强的而且是一个极不自然的限制. 更重要的是，这样一个限制不久就使得群论与它的一些邻近数学部门之间发生矛盾：在几何学的各个分支，自守函数以及组合拓扑学的理论中，常常遇到这样的一些代数对象，它们与群非常类似，只不过是无限的. 于是就对群论提出了有限群论所无法满足的要求. 同时，群论作为代数学的一部分，从代数学本身的观点来看，例如象整数加法群这样简单而又重要的群竟被排除在群论范围之外，

1) 在本书第三版问世前的年代里有限群论经历了蓬勃的发展——见补充的引言

也不能认为是正常情况. 因此, 有限群应该被看作群的一般概念的一个特殊情形, 而有限群论应该是一般"无限"(即不一定有限)群论中的一个篇章.

在世界文献中, 不假定有限性而叙述群论基础的第一本书是О. Ю. Шмидт的《抽象群论》(基辅, 1916), 这本书直到现在仍然是苏联一切代数工作者的常备参考书. 然而, 一般群论的广泛发展则开始得较晚, 这是在本世纪20年代随着代数里所进行的彻底的重新整理以及向集合论基础上的过渡 (E. Noether) 而一起开始的. 特别, 从此在群论中引入了象运算子系和链中断条件这样一些新的概念.

自此之后, 一般群论方面的工作有蓬勃的并且是多方面的开展, 现在这一数学分支已经成为一门范围广泛的内容丰富的科学, 是近世代数学中占首要地位的分支之一. 一般群论的发展自然不能忽视在有限群论中已经取得的成果. 相反地, 一般群论的发展在很多地方正是被有限群论中相应理论所推动的. 这里所遵循的原则是, 期望用一些自然的限制来代替群的有限性, 使得已知的定理和理论仍旧保持正确, 而去掉这些限制后即不再成立. 然而也常常出现这样的情形, 一些在有限群论里是非常简单并且被完全解决了的问题在一般群论里变成一个广泛发展并且还远没有完成的理论, 例如, 近代群论的重要分支之一的阿贝尔群论就是如此. 同时也产生了一些和无限群的研究本质地关联着的分支——自由群和自由积的理论. 最后, 在某些情形——首先是关于用定义关系给出群的问题中——, 群论第一次达到了在它以前的发展阶段所没有达到的精确和严格的程度.

群论离着完成还差得很远. 它的具体问题的多种多样性以及这样一些仅在最近才开始发展的方向的存在, 使我们可以认为, 一般群论还没有达到它本身发展的顶峰. 虽然如此, 把已经积累的

材料加以系统整理，以便使广大的数学工作者了解近代群论的主要方向，它的方法，它的最卓越的成就，最后还有它的当前的问题和最近发展中的必要途径，是适时的.

自然，本书并不打算包括群的全部理论，但是在这里几乎提供了这一门科学的一切基础部分，这些内容已经足够使读者看到这一理论内容的丰富性和方法的多样性.

本书并不要求读者具备关于群论基本概念方面的预备知识.只是为了作为群的某些最初的例子——矩阵，置换，单位根——才要求高等代数的基础知识. 要求读者关于数论方面的知识也只限于同余式的初步理论. 此外，关于集合论的基础知识方面，要求读者具备Hausdorff《集论》前四章的内容. 特别，许多构造和证明从本质上说要用到超限归纳法.

莫斯科，1940年10月.

上 册 目 录

第一篇　群论基础

第二篇 阿贝尔群

第一篇 群论基础

第一章 群的定义

§1. 代数运算

在高等代数课程中,读者就已遇到过带有代数运算的集合.高等代数中的主要集合是域和环，即带有两个独立运算(加和乘)的集合. 可是在各种各样的应用中都时常可以遇到那样一种集合,在它们里面只定义了一种代数运算（或者在该场合只考虑一种运算). 现在我们来说一下这个概念的定义.

设已知一集合 M. 如果对于集合 M 中按一定次序取出的任意两个(相同或不相同的)元素，根据某一规律可使属于同一集合中的完全确定的第三个元素和它们相对应，那我们就说，在集合 M 里面定义了一个代数运算.[1)]

因此,在代数运算的定义中,已经包括了运算的单值性的要求和对任意一对元素均可进行运算的要求. 另一方面，这个定义里还提到了进行运算时从集合 M 中取出元素的次序. 换句话说,这个定义并没有排除下述的可能性,即与集合 M 中的元素偶 a,b 及元素偶 b,a 相对应的元素可能互不相同,也就是说,所讨论的运算是非交换的.

可以举出许许多多由普通的数所组成的、带有一个运算的集

1）带有一个满足结合律的代数运算的集合 M 叫做一个半群.

合，它们能适合上述的定义．我们建议读者自己去造出一些这样的例子．在这里我们只指出，例如，负整数的集合对于乘法，奇数的集合对于加法是不适合我们的定义的．同样，全体实数的集合，如果把除法看作它上面的运算，也不适合这个定义，因为不能用零除．

如大家所熟知的，也有各种各样不是行之于数的代数运算的例子．n 维矢量空间中矢量的加法，三维欧氏空间中矢量的矢量乘法，n 阶方阵的乘法，一个实变数的实函数的相加以及这些函数的相乘等等，都是这样的代数运算．对以后来说一个非常重要的代数运算的例子，就是*置换的乘法*．如大家所知道的，所谓一个 n 次置换，就是头 n 个自然数集合的一个自身相互单值映射．相继进行两个 n 次置换，其结果仍旧是一个 n 次置换，叫做第一个置换乘上第二个置换的*乘积*．举例来说，如果给出当 $n=3$ 时的两个置换

$$a=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},\quad b=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},$$

那末这两个置换的乘积就是置换

$$ab=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}.$$

这样，在 n 次置换的集合中，就定义了一个代数运算．很容易看出，这个代数运算是非交换的；譬如对上面所给的那两个置换 a 和 b 来说，b 乘上 a 的乘积将是

$$ba=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}.$$

在研究带有一个代数运算的集合时，我们照例使用乘法的术语和记号．就是说，把所研究的运算叫作*乘法*，把对元素偶 a, b 进行运算的结果叫作这两个元素的*乘积* ab．但在某一些场合下，使

用加法的术语和记号要来得方便一些，那就是说，把运算叫作加法，而把运算的结果叫作元素 a,b 的和 $a+b$.

我们已经指出过，在代数运算的定义中，并没有要求运算是交换的，也就是说，并没有要求对集合 M 中的任意一对元素 a 和 b，等式

$$ab=ba$$

成立.

非交换运算的例子有：当 $n\geqslant 2$ 时 n 阶方阵的乘法，n 次置换的乘法，不仅对 $n=3$ 的情形是非交换的，如在上面已指出过的，对所有 $n\geqslant 3$ 的情形也都是非交换的. 此外，三维欧氏空间中矢量的矢量乘法也是非交换的. 数的减法也可以看作非交换运算的一个例子.

代数运算的定义并没有要求这个运算必须是结合的，也就是说，没有要求对集合 M 中的任意三个元素 a,b,c 等式

$$(ab)c=a(bc)$$

成立.

三维欧氏空间中矢量的矢量乘法是非结合运算的一个例子；整数的减法也是非结合的. 另一方面，如大家所知道的，方阵的乘法是结合的. 置换的乘法也是一个结合的运算，这一点可以从下面这个更普遍的结果中得出来.

设已知一个集合 S，有限或无限在所不论. 试考察所有将集合 S 映入其自身的单值映射. 也就是说，所有这样的映射，它们中的每一个能使 S 中的任意一个元素，都有这一集合中一个完全确定的元素和它相对应，虽然和 S 中不同元素相对应的元素可能是同一元素，并且在 S 中还可能有一些元素，谁也不和他们相对应. 如果我们把接连作这样两个映射的运算称为它们的相乘，那末我们就可以得出这个映射集合中的一个结合的代数运算.

事实上，设给出三个将集合S映入其自身的单值映射φ，ψ和χ. 其次，设a是集合S中的一个任意的元素，并设元素a被φ映到元素b，而元素b又被ψ映到元素c，最后，元素c又被χ映到元素d. 在这样的情形下，映射$\varphi\psi$将元素a映到元素c，因而映射$(\varphi\psi)\chi$将元素a映到元素d. 但映射$\psi\chi$将元素b映到元素d，因而映射$\varphi(\psi\chi)$也将元素a映到元素d. 这就证明了$(\varphi\psi)\chi$和$\varphi(\psi\chi)$这两个映射是一致的.

现在让我们来看一看，从某一集合M中给定的代数运算满足结合律这一事实可以推出怎样一些结论. 从代数运算的定义可知，从集合M中按一定次序取出的任意两个元素都有乘积，并且这个乘积是唯一确定的. 但仅仅根据这一点，在一般情形下我们还不能讨论三个元素的乘积——一般说来，依一定次序从M中取出的三个元素a，b和c，其乘积要看我们是怎样将它们相乘才能决定：是将a和b的乘积乘上c呢，还是将a乘上b和c的乘积？有了结合律，我们才可以唯一地说出M中三个元素的乘积：元素$(ab)c$等于元素$a(bc)$，并将其简单地记作abc. 显然，改换因子的次序时，三个元素的乘积一般说来也是会跟着改变的.

除此之外，有了运算的结合律，我们还可以谈论集合M中按一定次序取出的任意有限多个元素的乘积而不会有所误解. 也就是说，从结合律可以证明进行运算的结果与最初括号的分布位置无关. 现在让我们假定这一事实对因子的个数小于n的情形已经证明，进而来证明它对n个因子$(n>3)$的情形也成立. 设在已知集合M中有一个n个元素的有序组

$$a_1, a_2, \cdots, a_n,$$

在这些元素之间按某种方式安置了一些括号，表示运算进行的次序. 按这些括号所指示的次序依次相乘，最后一步，我们将把最先i个元素的乘积$a_1a_2\cdots a_i(1\leqslant i\leqslant n-1)$与乘积$a_{i+1}a_{i+2}\cdots a_n$相乘.

因为这两个乘积中因子的个数都小于 n，故根据我们的假定，它们是唯一地确定了的. 因此我们只要证明由乘积 $(a_1a_2\cdots a_i)(a_{i+1}a_{i+2}\cdots a_n)$ 可以过渡到乘积 $(a_1a_2\cdots a_j)(a_{j+1}a_{j+2}\cdots a_n)$，$i\neq j$，就行了. 很显然，后面这一事实只要就 $j=i+1$ 的情形来证明就够了，这是可以简单地运用结合律而达到的：如果

$$a_1a_2\cdots a_i=b,\quad a_{i+2}a_{i+3}\cdots a_n=c,$$

则

$$b(a_{i+1}c)=(ba_{i+1})c.$$

很显然，我们没有权利用上面的方法，来讨论 M 中无限多个元素的乘积.

有代数运算的集合 M，有时候也可能具有单位元素（或简称单位元），即这样一个元素 1，它使得等式

$$a\cdot 1=1\cdot a=a$$

对 M 中所有元素 a 都成立. 集合 M 里只可能有一个元素，具有这种性质：如果还可以找到第二个单位元素 $1'$ 的话，那末乘积 $1\cdot 1'$ 将会同时等于 1 和 $1'$，因而 $1=1'$. 在采用加法的记号时，单位元素将被称作零，并记作 0.

没有单位元素（或零）的带有代数运算集合的例子有：对于加法运算的自然数集合，对于乘法运算的偶数集合，以及对矢量乘法运算的三维欧氏空间中矢量集合. 另一方面，正如大家所知道的，n 阶方阵的乘法是有单位元素的，这个元素就是单位方阵. n 次置换的乘法也具有单位元素，不难看出，这个元素就是恒等置换

$$\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}.$$

一般地说，在将某一集合 S 映入其自身的全部单值映射的集合中，如果把映射的相继进行当作乘法的话，集合 S 的恒等自身映射就是单位元素.

最后，让我们引入逆运算这个概念. 从高等代数的课程中我们知道，在任意一个环里面，减法是加法的逆运算；而在任意一个域里面，如果只考虑不等于零的元素的话，那末除法就是乘法的逆运算. 按照这两个例子，对任意一个带有一个代数运算(不一定是可换的)的集合 M，可以很自然地提出这样一个问题：对于 M 中两个已知的元素 a 和 b，可否找到这样两个元素 x 和 y，使

$$ax=b, \quad ya=b. \tag{1}$$

这两个方程可能在集合 M 内没有解. 另一方面，每一个方程都可能在 M 里有许多个互不相同的解. 如果对任意的 a 和 b，方程(1)中的每一个都有解，并且这个解是唯一的，那我们就说，*在集合 M 中所定义的运算具有逆运算*. 很显然，在非交换运算的情形，这两个解不一定相等.

任意一个有零因子的环(例如函数环和方阵环)里的乘法，是使方程(1)可能具有几个不同的解的运算的例子. 使方程(1)不永远有解的运算的最简单的例子，是自然数集合中的加法以及整数环中的乘法. 对实数域中的乘法来说也是如此，这是因为不能用零除的缘故.

§2. 同构·同态

设已知两个集合 M 和 M'，每一个集合里面都定义了一个代数运算. 我们将把这两个集合里的运算都叫作乘法. 设在集合 M 和 M' 的元素之间可以建立一个相互单值的对应，具有下面的性质：如果与 M 中的元素 a, b 相对应的 M' 中的元素是 a', b'，且

$$ab=c, \quad a'b'=c'$$

则在这个对应下，与集合 M 中的元素 c 相对应的，不是 M' 中任何其他元素而恰是元素 c'. 在这样的情形下，我们就说集合 M 和 M' *同构*. 这样一个相互单值的对应，我们称作集合 M 和 M' 之

间的同构对应. 集合 M 和 M' 同构这个事实，我们用记号

$$M\simeq M'$$

来表示.

要举出相互同构的、带有一个代数运算的集合的例子并不困难. 举例说，如果对于每一个偶数 $2k$，我们使整数 $3k$ 和它相对应，那就可以在偶数的集合和 3 的倍数的集合之间建立起一个相互单值对应. 对于在这两个集合中定义的加法来说，这个对应就是一个同构对应.

现在让我们来比较一下正实数集合中的乘法运算和全部实数集合中的加法运算. 如果对于每一个正实数，我们使这个数的以 10 为底的对数和它相对应，那末我们就可以得到一个相互单值的映射，将第一个集合映成第二个集合. 等式

$$\log(ab)=\log a+\log b$$

表明，这映射是一个同构映射.

从高等代数课程中也可以找出许多同构集合的例子来. 下面我们提一下其中的一个：在某一域 P 上的 n 维矢量空间的线性变换的集合，把线性变换的相继施行当作它们的乘法. 这个集合和以方阵乘法当作代数运算的域 P 上 n 阶方阵的集合同构. 大家知道，这两个集合间的同构对应和矢量空间的基的选择有关. 因此，如果各带一个代数运算的两个集合 M 和 M' 同构的话，一般说来，它们之间的同构对应可以用多种不同的方法来建立.

很显然，每一个带代数运算的集合都与它自身同构：只要取这个集合的恒等自身映射当作同构映射就行了. 其次，同构关系是对称的——由 $M_1\simeq M_2$ 即可得出 $M_2\simeq M_1$，它也是传递的——由 $M_1\simeq M_2$ 和 $M_2\simeq M_3$ 即可得出 $M_1\simeq M_3$.

从同构的定义还可以看出，相互同构的集合有相同的势. 特别是，当这些集合都是有限的话，那末它们必是由同样多个元素

组成.

相互同构的带有代数运算的集合之不同处，只在于其元素的性质不同，或是因为运算的名称和用来表示运算的符号不一样.但从运算的性质来看，他们是全没有区别的:即对于带运算的某一集合，凡是可以根据这运算的性质而不必利用元素的特性来证明的那些结论，都可以自动地转移到所有和这个集合同构的集合上去.因此，在今后我们将把相互同构的集合看作是带同一运算集合的不同样品，这样我们就将代数运算划分出来作为真正的研究对象.只有在造各种各样的具体例子的时候，我们才不得不讨论具体的集合以及根据这些集合中元素的特性来定义的运算.顺便提一句，在后面(在第五章里)我们将学会怎样给出运算的具体例子，而不必对在其上进行运算的元素的特性作任何假定.

同构概念并不是代数学所特有的概念. 事实上，任何一门数学科学都会按照某些特征将它所研究的对象等同起来，并通过这一方式将这一学科的对象的性质突出地表现出来.要了解这一点，读者只要想一下，最基本的数学概念之一——整数的概念是怎样建立起来的就行了.

如果从同构的定义中去掉相互单值这一要求，我们就可以得出同构概念的一个推广. 设已知两个集合 M 和 M'，各带有一个代数运算——乘法. 试考察将 M 映到 M' 上的映射 φ，在这个映射下，M 里的每一个元素 a 都有 M' 里一个完全确定的象元素 $a'=a\varphi$ 和它相对应，并且 M' 里的每一个元素在 M 里至少有一个原象，但一般说来可能有许多不同的原象. 如果对于 M 里的任意两个元素 a 和 b，由

$$a\varphi=a',\quad b\varphi=b'$$

即可得出

$$(ab)\varphi=a'b',$$

这个映射就称为一个同态映射. 我们也说，集合 M' 是集合 M 的一个同态象.[1]

很显然，如果一个集合可以同态地映到另一集合上的话，并不能把它们看成完全相同. 因此，同态概念的作用不如同构概念那样具有根本性意义，可是在整个理论的进一步发展中，这个概念的作用也是很重要的. 现在让我们举出几个同态映射的例子.

设 M 是全体整数的集合，以加法作为代数运算；M' 是由 1 和 -1 这两个数所组成的集合，以乘法作为代数运算，这个运算在它里面显然是可以定义的. 使 1 和每一个偶数相对应，-1 和每一个奇数相对应，我们就可以得出一个将 M 映到 M' 上的同态映射. 事实上，"偶数加奇数等于奇数"这一规则对应于等式 $1\cdot(-1)=-1$. 余类推.

设 M 是在平面上由坐标原点出发的全部矢量的集合，M' 是位于横坐标轴上的全部矢量的集合；而且在两个集合中代数运算都取作矢量加法. 如果对 M 中的每个矢量，都使它在横坐标轴上的投影和它相对应，我们就得出一个将 M 映到 M' 上的同态映射，这是因为，两个矢量的和在横坐标轴上的投影，等于这两个矢量的投影的和.

如果带一个代数运算的集合 M 可以同态地映到集合 M' 上，特别是，如果这两个集合同构，那末由结合律或交换律在 M 中成立可以推出相应的规律在 M' 中也成立. 举例来说，设 M 中的运算适合交换律. 如果 a' 和 b' 是 M' 中两个任意的元素，a 是元素 a' 在集合 M 中的原象之一，b 是元素 b' 的原象之一. 那末在这个同态映射下，元素 $a'b'$ 和元素 ab 对应，元素 $b'a'$ 和元素 ba 对应. 因此，由等式 $ab=ba$ 及在同态映射下象元素的唯一性可得出 $a'b'$

---

1) 有关同态的某些新的术语在补充 2.1 里指出.

$=b'a'$. 在集合 M 中的运算适合结合律的情形，其证明可按同样的方式来进行.

其次，如果集合 M 有单位元素 1，那末这个单位元素的象元素就是集合 M' 中的单位元素. 我们用 e' 来表示元素 1 在 M' 中的象元素. 如果 a' 是 M' 中一个任意的元素，a 是它的原象之一，那末由等式 $a\cdot 1=1\cdot a=a$ 及映射的同态性质可得出等式 $a'\cdot e'=$ $=e'\cdot a'=a'$. 这样就证明了 e' 的确是集合 M' 中的单位元素.

注意，如果集合 M 具有逆运算，则对它的同态象 M' 不能下同样的断语. 因为我们不能证明上节(1)式中的每一个方程在 M' 中的解都是唯一的，虽然在这种情形我们仍能够证明这两个方程的确都有解.

事实上，设 a' 和 b' 是 M' 中的两个元素，a 和 b 分别是它们在 M 中的某两个原象，也就是说，

$$a\varphi=a',\quad b\varphi=b'.$$

如果元素 c 满足集合 M 中的方程 $ax=b$，那末由于映射 φ 的同态性质，元素

$$c'=c\varphi$$

将能满足 M' 中的方程 $a'x'=b'$.

另一方面，我们要指出，如果在集合 M' 中结合律或交换律成立，或在 M' 中单位元素存在，或 M' 中的运算具有逆运算，但对集合 M 不能推出同样的断语.

有一种方法可以用来确定带有一个代数运算的集合 M 的全部同态象. 为了这个目的，我们先引入下面的概念. 设集合 M 可按某种方式划分成为一些互不相交的子集，这些子集我们称为类，并用字母 $A, B,$ …来表示它们. 如果元素 a_1 和 a_2 属于同一类 A，元素 b_1 和 b_2 属于同一类 B，并由此可以得出乘积 a_1b_1 和 a_2b_2 也同样属于同一个类 C，那我们就说，集合 M 的这一划分是一个正

则分解.[1]

从这个定义可以看出：只要给出类A与B来，类C也就完全确定了——A中任意一个元素和B中任意一个元素的乘积包含在C内. 如果我们把类C称作类A和类B的乘积，那末在这个正则分解下的全部类的集合$\overline{M}$中，就定义了一个代数运算. 带有这个代数运算的集合$\overline{M}$，我们称作M对这一正则分解的商集.

集合M可同态地映到商集$\overline{M}$上. 事实上，只要使集合M中的每一个元素所在的类和这个元素相对应，并利用集合$\overline{M}$中乘法的定义就行了. 这个同态映射称为将集合M映到商集$\overline{M}$的自然同态映射.

集合M对不同正则分解的商集，实质上穷尽它的一切同态象. 更确切一点说，我们有下面这个定理：

如果M'是集合M的一个任意同态象，φ是将M映到M'上的同态映射，那末可以找到将集合M划分成不相交子集(类)的一个正则分解，使集合M'和集合M对这一正则分解的商集$\overline{M}$同构. 除此之外，在集合M'和$\overline{M}$之间还可以找到这样一个同构映射ψ，使相继进行映射φ和ψ的结果，和将M映成$\overline{M}$的自然同态映射相吻合.

为了证明这个定理，首先要指出：如果我们把集合M中在同态映射φ下有相同象元素的全部元素归作一个类，我们就可以得出一个划分，它将集合M分成为一些互不相交的子集. 这个划分是一个正则分解：如果元素a_1和a_2属于同一个类，即

$$a_1\varphi = a_2\varphi = a';$$

又若元素b_1和b_2属于同一个类，即

$$b_1\varphi = b_2\varphi = b',$$

1) 现在把正则分解的概念叫做同余.

那末由于映射φ的同态性质，就可得到：

$$(a_1b_1)\varphi=(a_2b_2)\varphi=a'b',$$

这就是说，元素 a_1b_1 和 a_2b_2 也属于同一个类．这样一来，我们就可以用上面所讲的方法，在这个划分下所得出的全部类的集合 $\overline{M}$ 中定义乘法，也就是说，把 $\overline{M}$ 变成一个商集．在集合 M' 的全部元素和集合 M 的全部类(即集合 $\overline{M}$ 的元素)之间，存在一个相互单值的对应 ψ—— 对于 M' 中的每一个元素，使由这个元素的全部原象所组成的类和它相对应．对应 ψ 是一个同构对应：如果与集合M' 中的元素 a', b' 相对应的两个类是A和B，并且从这两个类中各选出一个元素—— 从A中选出了元素 a，从B中选出了元素 b，那末 AB 就是包含元素 ab 的那个类．但

$$(ab)\varphi=(a\varphi)(b\varphi)=a'b',$$

故映射ψ使类 AB 和元素 $a'b'$ 相对应．为了结束这个证明，我们从 M 中取出一个任意的元素 a，设

$$a\varphi=a', \quad a'\psi=A.$$

因为元素 a 是元素 a' 的原象之一，故 a 包含在A内．这就是说，相继进行映射φ和ψ的结果，的确和将 M 映成 $\overline{M}$ 的自然同态映射相吻合．定理就被证明了．

§3. 群

进一步研究带一个任意代数运算的集合，将是一件很少成效的工作，因为这个概念实在是太广泛，因而也缺乏内容．在历史上，由于数学本身及数学以外的部门在应用上有所需要，于是划分出一类特别的带一个代数运算的集合，并对它进行了详尽的研究，这里指的就是所谓的*群*．这个概念是近代数学中最基本的概念之一，它兼备了下面两个优点：一方面跟数的运算非常相近，另一方面又有着广泛的应用范围．

带有一个代数运算的非空集合 G，如果满足下面两个条件，就叫做一个群：

1） G 里面的代数运算满足结合律；

2） 在 G 里面逆运算可以进行.

群 G 里面的代数运算不一定满足交换律. 如果这个运算满足交换律，群 G 就称为一个交换群或阿贝尔群. 阿贝尔 (Abel) 曾经研究过一类方程，它们的理论和交换群的理论有关. 很显然，这一类群中的运算和我们所习惯的数上的运算特别相近；在后面我们将用许多的篇幅来对阿贝尔群的性质作详细的研究.

如果在任意群 G 中，对某两个元素 a 和 b 交换律能满足，我们就说这两个元素可换.

如果群 G 是由有限多个元素组成的，那末这个群就称为有限群，它里面的元素的个数则称为这个群的阶. 在下一节里，我们将要证明任意阶的有限群及具有任意无限势的群存在.

对于有限群的情形，可以在群的定义的条件 2) 中只留下方程

$$ax=b, \quad ya=b \tag{1}$$

的解的唯一性这一项要求，也就是说，解的存在可以作为一项推论从解的唯一性推引出来. 事实上，设带一个代数运算的集合 G 是有限的，由 n 个元素组成，并设在这个集合里方程(1)的解，如果它们存在的话，是唯一地决定的. 今给出集合 G 中的两个元素 a 和 b. 将元素 a 从右边乘上 G 中的元素 x，即作乘积 ax，并命 x 遍历 G 中的全部元素. 这样一来，根据我们所作的假定，就可以得出 G 中 n 个不同的元素，也就是说，可以重新得出 G 中的全部元素. 因此，一定可以找到一个元素 x_0，使 ax_0 等于已给的元素 b. 这样，式(1) 中第一个方程的解的存在就被证明了. 第二个方程的解的存在可以用同样的方法来证明.

以加法作为运算的正整数集合的这个例子表明，在无限群的

情形，对条件 2)不能作类似的削弱．在正整数的集合里，加法运算是永远可以进行的，并且满足结合律；逆运算——减法——也是单值的，但不是经常都能进行．

现在让我们从群的定义出发，证明几条最简单的推论．

从群 G 中取出一个任意的元素 a．由条件 2)可知，群 G 中存在一个元素 e_a，使 $ae_a=a$，并且这样的元素是唯一的．当我们将元素 a 从右边乘上 e_a 时，e_a 这个元素起着单位元素的作用．事实上，元素 e_a 对群 G 中所有的元素都有这个性质：设 b 是群 G 中任意一个另外的元素，y 是群 G 中满足等式 $ya=b$ 的元素，由条件 2)可知 y 这样的元素是存在的．将等式 $ae_a=a$ 的两端同时从左边乘上 y，并将等式的左端运用结合律，我们就可以得出 $be_a=b$．这样，我们就证明了群 G 中*右单位元素* e' 的存在和唯一性．对 G 中所有元素 x，元素 e' 有性质：$xe'=x$．

用同样的方法可以证明群 G 中*左单位元素* e'' 的存在和唯一性．即对群 G 中所有元素 x，元素 e'' 满足条件 $e''x=x$．

事实上，元素 e' 和 e'' 是相等的，这可以由等式 $e''e'=e'$ 和 $e''e'=e''$ 看出．这样，我们就证明了任意一个群 G 中满足条件

$$xe=ex=x \text{（对群 } G \text{ 中的所有元素 } x\text{）}$$

的元素 e 的存在和唯一性．这个元素是群 G 的*单位元素*（参看§1)，我们用记号 1 来表示它．正如我们所看到的，单位元素和群中任意元素可换．

其次，从条件 2)还可以看出，对于一个已给的元素 a，可以找到两个元素 a' 和 a''，使其满足条件

$$aa'=1,\quad a''a=1,$$

并且这样的元素是唯一确定的．事实上，a' 和 a'' 这两个元素是相等的：由

$$a''aa'=a''(aa')=a''\cdot 1=a''$$

和

$$a''aa'=(a''a)a'=1\cdot a'=a'$$

可知 $a''=a'$. 这个元素我们用记号 a^{-1} 来表示，并把它叫做元素 a 的逆元素. 因此，对群 G 中的任何一个元素 a 都存在一个唯一确定的逆元素 a^{-1}，适合条件

$$aa^{-1}=a^{-1}a=1.$$

从上面这个等式还可以看出，元素 a^{-1} 的逆元素就是元素 a 本身，也就是说，$(a^{-1})^{-1}=a$，且每一个元素和它自己的逆元素可换. 其次，很容易验证，几个元素的乘积的逆元素，等于各个因子的逆元素按相反的次序的乘积，即

$$(a_1a_2\cdots a_{n-1}a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}.$$

单位元素的逆元素，就是单位元素本身.

利用逆元素这个概念，就可把根据条件 2)而存在的适合等式 $ax=b$ 和 $ya=b$（a 和 b 是已知的元素）的那两个元素 x 和 y 用明显的形式写出来. 事实上，经过直接的验算就可以看出

$$x=a^{-1}b,\quad y=ba^{-1},$$

从这里还可以看出，在非交换群的情形，x 和 y 可能是群中互不相同的元素. 很显然，在阿贝尔群的情形这是不可能的.

逆元素的存在和唯一性，我们是从条件 2) 中推出来的. 而事实上，反过来又可以用这些事实来代替条件 2). 我们现在就来证明这一点，并且在证明的时候甚至还可以不假定单位元素和逆元素的唯一性，只要假定它们的一侧存在（譬如说右侧存在）就行. 把条件 2) 作这样的削弱，有时候能够使我们便于验证一个已知的带运算集合是不是一个群.

如果 G 是一个带有满足结合律的运算的集合，那末条件 2) 可由下面两个条件中推出:

2′) G 中至少存在一个右单位元素 e，具有性质

$$ae=a \quad (\text{对 } G \text{ 中所有元素 } a);$$

2″)在 G 的右单位元素当中有这样一个元素 e_0，使对 G 的任意一个元素 a 至少可以找到一个*右逆元素* a^{-1}，具有性质

$$aa^{-1}=e_0.$$

证明：设 a^{-1} 是元素 a 的右逆元素之一．将等式 $aa^{-1}=e_0$ 的两端同时从左边乘上 e_0，我们就得出

$$e_0aa^{-1}=e_0e_0=e_0,$$

由此即有

$$e_0aa^{-1}=aa^{-1}.$$

将这个等式的两端同时从右边乘上 a^{-1} 的逆元素之一，就可以得出

$$e_0ae_0=ae_0,$$

由此即有 $e_0a=a$．这样一来，e_0 也是 G 中的左单位元素．

现在设 e_1 是一个任意的右单位元素，e_2 是一个任意的左单位元素．由等式

$$e_2e_1=e_1 \text{ 和 } e_2e_1=e_2$$

可得出 $e_1=e_2$．这样就证明了单位元素的唯一性．

将等式 $aa^{-1}=e$ 的两端同时从左边乘上 a^{-1}，我们可得到

$$a^{-1}aa^{-1}=a^{-1}.$$

再将这个等式的两端同时从右边乘上 a^{-1} 的逆元素之一，就可以得出 $a^{-1}a=e$，这就是说，元素 a^{-1} 同时也是 a 的左逆元素．现在如果 a_1^{-1} 和 a_2^{-1} 分别是元素 a 的任意的右逆元素和左逆元素，那末由等式

$$a_2^{-1}aa_1^{-1}=(a_2^{-1}a)a_1^{-1}=a_1^{-1},$$

$$a_2^{-1}aa_1^{-1}=a_2^{-1}(aa_1^{-1})=a_2^{-1},$$

可知 $a_1^{-1}=a_2^{-1}$，也就是说，逆元素存在且是唯一的．

现在就可以毫不费力地来证明条件 2)了．为了满足方程

$$ax=b, \quad ya=b,$$

只要令 $x=a^{-1}b$ 和 $y=ba^{-1}$ 就行. 这个解的唯一性, 例如对第一个方程来说,可以由下面的事实看出来: 如果 $ax_1=ax_2$ 的话,那末将等式两端同时从左边乘上 a^{-1} 之后即得出 $x_1=x_2$.

注意,利用方程(1)的解的唯一性, 可以进行*左侧的和右侧的消去法*: 如果

$$ab_1=ab_2 \quad \text{或} \quad b_1a=b_2a,$$

则 $b_1=b_2$.

如果群 G 可以同态地(或同构地)映到带一个代数运算的集合 G' 上,那末 G' 也是一个群.

事实上, 由上节中所证明的结果可知 G' 中的运算满足结合律. 方程(1)在 G' 中有解, G 中的单位元素的象元素是 G' 中的单位元素. 因此, 在集合 G' 中条件 2′)和 2″)能满足,因而根据以上所证,G' 是一个群.

特别是, 群 G 对它的任意一个正则分解的商集是一个群. 因此,在以后我们可以说群 G 对其正则分解的*商群*.

上节末所证明的那个定理, 在群的情形变成下面这个非常重要的同态定理:

如果 φ 是一个同态映射, 将群 G 映成群 G', 那末一定可以找到群 G 的一个正则分解,使群 G' 可以同构地映到群 G 对这一分解的商群 $\overline{G}$ 上. 除此之外, 将 G' 映到 $\overline{G}$ 上的同构映射 ψ 还可以这样选择, 使相继进行映射 φ 和 ψ 的结果刚好和将群 G 映到商群 $\overline{G}$ 上的自然同态映射相吻合.

关于同态映射,我们还要作一个按语.

如果将群 G 映到群 G' 上的同态映射 φ 将 G 中的元素 a 映到 G' 中的元素 a':

$$a\varphi=a',$$

则元素 a^{-1} 的象元素将是元素 a'^{-1}:

$$a^{-1}\varphi=a'^{-1}.$$

事实上,我们知道 $1\varphi=1'$. 如果令 $a^{-1}\varphi=b'$,就有

$$1\varphi=(aa^{-1})\varphi=a\varphi\cdot a^{-1}\varphi=a'b',$$

也就是说,$a'b'=1'$,由此即有 $b'=a'^{-1}$.

元素的阶 群G中与元素a相等的n个元素的乘积,称为元素a的n次幂,记作a^n. 元素a的负幂可以定义为元素a的正幂在群G中的逆元素,或若干个与元素a^{-1}相等的元素的乘积. 事实上,这两个定义是彼此吻合的:

$$(a^n)^{-1}=(a^{-1})^n.$$

要证明这个等式,只要作$2n$个因子的乘积,其中前n个因子都等于a,其余n个因子都等于a^{-1},然后依次抵消就行. 元素a的负幂我们记作a^{-n}. 最后,我们约定将a^0理解作元素1.

很容易验证,对于任意正的,负的或等于零的指数n和m,等式

$$a^n\cdot a^m=a^m\cdot a^n=a^{n+m},$$

$$(a^n)^m=a^{nm}$$

成立. 第一个等式表明,同一元素的各次幂彼此可换.

如果元素a的所有各次幂都是互不相同的元素,那末就称a为一个无限阶元素. 现在设元素a的各次幂中有相等的元素,譬如说,$a^k=a^l$而$k\neq l$. 特别在有限群的情形这样的情况是一定会出现的. 如果$k>l$,则$a^{k-l}=1$,也就是说,元素a有等于1的正幂. 设n是使得a的幂等于1的最小的正整数,也就是说,设

1) $a^n=1, n>0$;

2) 如果 $a^k=1, k>0$, 则 $k\geqslant n$.

在这样的情形我们就说,a是一个有限阶元素,它的阶等于n.

如果元素a的阶等于n,那末很容易看出,所有元素

$$1, a, a^2\cdots, a^{n-1}$$

都互不相等. 元素 a 的任何另外一个幂，不论是正幂或负幂，都必定和些这元素当中的一个相等. 事实上，设 $k=nq+r$, $0\leqslant r<n$. 于是就有

$$a^k=(a^n)^q\cdot a^r=a^r.$$

从这里还可以看出，如果元素 a 的阶是 n 而 $a^k=1$ 的话，那末 k 一定可以被 n 整除.

每一个群都有一个唯一的 1 阶元素，这就是单位元素 1. 有限 n 阶元素 a 的逆元素，显然就是元素 a^{n-1}.

在一个有限群里，所有元素的阶都是有限的. 在 § 4 里，我们将要证明也存在这样的无限群，其所有元素都是有限阶的. 所有元素都是有限阶的群称为*周期群*. 另一方面，也存在那样一种群，在它们里面除单位元素之外，所有元素的阶都是无限的. 这样的群习惯叫作*无扭群*. 最后，如果一个群里面既包含无限阶元素，也包含不等于单位元素的有限阶元素，这样的群就可以很自然地称为*混合群*.

如果把群 G 中的运算称做*加法*，那末对于前面的术语和记号也应作某种改变. 在这种情况，正如 § 1 所提到过的，我们不说群里面有单位元素，而说它里面有*零元素*，并记作 0. 除此之外，元素 a 的逆元素我们将称做它的*负元素*，并记作 $-a$. 我们也不再说元素 a 的幂，而改称做它的*倍元素*，并把它们记作 ka.

§3a Baer 和 Levi 的公理体系

在 § 3 里已经指出，群可以用不同的方式来定义. 关于群的定义用公理来刻画的各种问题——足以定义群的尽可能弱的公理的问题，公理的独立性问题等等——在 20 世纪初叶，引起了许多数学家，其中多数是美国数学家 (Moor, Hantington, Dickson) 的

兴趣. 在这个课题上的研究出现得晚一些，现在还时有出现. 最为完整的结果要算是 Baer 和 Levi[1]，我们将在这一节里加以阐述[参看补充 1. 1.].

在§3 的开始所给出的群的定义，实际上由七条公理组成：三条存在公理——乘积和两侧商的存在，三条相应的唯一性公理以及结合公理. 这些公理彼此独立地被表述如下.

在集合 G 里，三个(有序的)元素，a, b, c 由关系

$$a=bc \tag{1}$$

联系着. 用语言表述就是：a 是 b 乘 c 的乘积，b 是元素 a 与 c 的左商，c 是元素 a 与 b 的右商. 集合 G 是一个群，如果下列条件被满足：

E_a. 对于给定的 b 和 c，至少存在一个 a，满足条件(1).

E_b. 对于给定的 a 和 c，至少存在一个 b，满足条件(1).

E_c. 对于给定的 a 和 b，至少存在一个 c，满足条件(1).

U_a. 对于给定的 b 和 c，至多存在一个 a，满足条件(1).

U_b. 对于给定的 a 和 c，至多存在一个 b，满足条件(1).

U_c. 对于给定的 a 和 b，至多存在一个 c，满足条件(1).

A. 如果在 G 里存在形如 $(a_1a_2)a_3$ 的元素，又存在形如 $a_1(a_2a_3)$ 的元素，那末这两个乘积确定这个集合里同一个元素.

结合公理 A 的表述不包含任何关于存在性和唯一性的断言. 特别，这种表述允许乘积 $(a_1a_2)a_3$ 和 $a_1(a_2a_3)$ 中的一个在 G 内有定义，而另一个没有定义.

上述七条公理中的一部分叫做一个*完备系*，如果这一部分公理即足以定义群，也就是说，如果其余的公理都可以由这一部分推导出来. 一个完备的公理系说是*极小的*，如果从其中去掉任何一条后，都不再是完备系. 我们的任务就是要建立群的公理的一切极小完备系.

今后为了方便起见，把上述前六条公理排成矩阵的形式

$$\begin{pmatrix} E_a & E_b & E_c \\ U_a & U_b & U_c \end{pmatrix}. \tag{2}$$

设 Σ 是公理的一个完备系. 那末 Σ 具有下列性质 1—4:

1. Σ 包含结合公理 A.

事实上，取由三个元素 a, b, c 所组成的集合，按以下的表在其中定义乘法：

	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

象通常那样，元素 x 乘以元素 y 所得的乘积记在 x 所在的行与 y 所在的列的交点处. 元素 a，b, c 中每一个恰在每一行和每一列中出现一次，因此，矩阵(2)里所有的公理都成立. 然而结合公理不成立: $(ab)c=c$ 但 $a(bc)=b$.

2. Σ 至少包含矩阵(2)的每一行和每一列中一条公理.

下面关于定义在含有两个元素 a，b 的集合上的运算的例子表明，矩阵(2)的任意一行或任意一列中的公理独立于其余的公理:

	a	b
a	—	—
b	—	—

	a	b
a	(a,b)	(a,b)
b	(a,b)	(a,b)

	a	b
a	a	a
b	b	b

	a	b
a	a	b
b	a	b

	a	b
a	—	(a,b)
b	(a,b)	—

这里记号 (a,b) 表示运算结果是两个元素 a 和 b，而记号—表示没有乘积.

在所有这五个例子里，公理 A 都成立；在第一个例子里公理

U_a, U_b, U_c 成立；在第二个例子里 E_a, E_b, E_c 成立；在第三个例子里 E_a, E_b, U_a, U_b 成立；在第四个例子里 E_a, E_c, U_a, U_c 成立；在第五个例子里 E_b, E_c, U_b, U_c 成立，而在每一个例子里，其余公理不成立.

3. Σ 至少包含矩阵(2)的第一行中两条公理.

自然数加法的例子说明公理系 E_a, U_a, U_b 和 U_c 的不完备性. 以下所作的例子说明，任何一个公理系，如果在矩阵(2)的第一行里只包含公理 E_b，一定是不完备的.

首先考虑自然数的一切序对的集合. 按自然数列的序型赋与这个集合一个次序，对于两个对(i_1, j_1)和(i_2, j_2)来说，一个对被认为先于另一个对，如果它里面的较大元素小于另一个对里面的较大元素；具有同一个较大元素的对——对于给定的较大元素，这样的对只有有限个——，随意地给它们排定一个次序. 例如，自然数对的集合可以如下给予次序：

$(1,1), (1,2), (2,1), (2,2), (1,3), (3,1), (2,3), (3,2), (3,3), \cdots$

以自然数按其通常次序用上法排定次序的元素对编上号，但从 2 开始. 元素对(i, j)的号码用$[i, j]$表示. 在上面所给的例子里就是

$$[1,1]=2, [1,2]=3, [2,1]=4, [2,2]=5, \cdots$$

容易确信，对于任意 i 和 j，存在着严格不等式

$$[i, j]>i, \quad [i, j]>j. \tag{3}$$

现在可以如下构造所求的例子. 取一个可数集，它由元素

$$a_1, a_2, \cdots, a_n, \cdots$$

组成. 令

$$a_{[i,j]}a_i = a_j. \tag{4}$$

这样定义的乘法不满足公理 E_a，因为不能用元素 a_1 从左边去乘；

又因为当 $\alpha\leqslant\beta$ 时，$a_\alpha x=a_\beta$ 没有解，所以 E_c 也不成立．然而容易看出，公理 E_b，U_a,U_b,U_c 都被满足．从上面注释，即在我们的例子里，乘积 $a_\alpha(a_\beta a_\gamma)$ 和 $(a_\alpha a_\beta)a_\gamma$ 不能同时存在，所以公理 A 成立．事实上，每一个元素至多可能是一个乘积的左因子．因此，如果乘积 $a_\alpha(a_\beta a_\gamma)$ 和 $a_\alpha a_\beta$ 都存在，那末必须 $a_\beta a_\gamma=a_\beta$；然而由(3)和(4)，这是不可能的．

根据左除与右除的对称性，可以类似地证明，在矩阵(2)的第一行里只包含公理 E_c 的公理系也是不完备的．

4. Σ 或者包含关于除法存在的两个公理 E_b 和 E_c，或者包含除法唯一性的两个公理 U_b 和 U_c．

根据上面所证明的性质 2，我们只需证明，或者公理系 A,E_a,E_b,U_a,U_c 是不完备的，或者公理系 A,E_a,E_c,U_a,U_b 是不完备的．我们只对第一个公理系来证明，对第二个公理系的证明可以利用对称性得出．

令 B 是一个可数无限集．令 M 表示 B 的一切这样的无限子集 B' 所成的集合：B' 在 B 中的余集 B/B' 也是无限的．每一个子集 B' 也是可数的，从而可以通过多种方式与 B 建立相互单值映射．对于 M 的一切 B'，一切这样的映射所成的集合记作 Φ．在集合 Φ 里，定义代数运算如下：如果 φ_1 和 φ_2 是 Φ 的两个元素，它们分别将 M 中的 B'_1 和 B'_2 映到 B 上，那末 B'_1 包含一个子集 B'_{12}，它通过 φ_1 映到 B'_2 上，从而依次施行映射 φ_1 和 φ_2，B'_{12} 被映到 B 上．我们把 B'_{12} 到 B 上的这个相互单值映射记作 φ_{12}，并且定义为 φ_1 与 φ_2 的乘积：

$$\varphi_{12}=\varphi_1\varphi_2.$$

映射 φ_{12} 属于集合 Φ，因为集合 B'_{12} 属于 M．事实上，余集 B/B'_{12} 包含余集 B/B'_1，因而是无限集；而 B'_{12} 本身也是无限集．

在集合 Φ 里这样定义的运算显然满足 E_a 与 U_a．容易验证这

个运算是结合的．我们证明公理 E_b 和 U_c 成立．设任意给定Φ中两个元素 φ_2 和 φ_{12}，它们分别将 B'_2 和 B'_{12} 映到 B 上．设 b 是 B 中任意元素．分别用 b_2 和 b_{12} 表示 B'_2 和 B'_{12} 中这样的元素，它们在映射 φ_2 和 φ_{12} 之下被映成 b．然后取这样一个子集 B'_1，使得$B'_{12}\subset B'_1\subset B$，并且两个余集 B'_1/B'_{12} 和 B/B'_1 都是无限的．令 φ_1 表示 B'_1 到 B 上这样一个相互单值映射，在这个映射之下，每一元素 b_{12} 被映成 b_2，而余集 B'_1/B'_{12} 通过某一种方式相互单值地映到 B/B'_2 上，那末 φ_1 属于Φ，并且等式 $\varphi_1\varphi_2=\varphi_{12}$ 成立．因此公理 E_b 成立；同时我们也看到，公理 U_b 不成立．

现在设给定了Φ中的任意元素 φ_1 和 φ_{12}，它们分别将集合 B'_1 和 B'_{12} 映到 B 上．满足方程 $\varphi_1 x=\varphi_{12}$ 的映射 φ_2 只有当 B'_{12} 含于 B'_1 内的时候才可能存在．因此公理 E_c 不成立．然而假设 φ_2 存在．如果给定 B 中元素 b，它是元素 b_{12} 在 φ_{12} 之下的象，而在 φ_1 之下，元素 b_{12} 被映成 b_2，那末元素 b_2 应该被 φ_2 映成 b．这就证明了在Φ中公理 U_c 成立．性质 4 证毕．

以上所证明的性质 1—4 合起来与公理系的完备性等价．我们有以下定理：

任意一个具有性质 1—4 的公理体系是完备的．

证明基于以下三条引理．

引理 1 *公理系 A, U_a, E_b, E_c 是完备的．*

设 d 和 d' 是所考虑的集合 G 的任意两个元素．根据 E_b 和 E_c，存在元素 e，f 和 g，使得 $ed=d, ef=d', dg=f$．于是

$$d'=e(dg),\qquad f=(ed)g.$$

右端两个表示式存在，并且根据 U_a，是唯一确定的．因此，根据公理 A，$f=d'$，从而 $ed'=d'$．元素 d' 是集合 G 的任意元素，所以 e 是 G 的一个左单位元．

其次，根据 E_b 和 E_c，存在这样的元素 d^{-1}，h 和 k，使得

$d^{-1}d=e, d^{-1}h=d', dk=h$. 于是

$$d'=d^{-1}(dk), \qquad k=ek=(d^{-1}d)k.$$

再由 U_a 和 A，我们得到 $k=d'$，即 $dd'=h$. 这就证明了任意两个元素乘积的存在，即公理 E_a 成立. 由左单位元和左逆元的存在就可以象 §3 里那样，证明 U_b 和 U_c.

引理 2 任何一个包含 A, E_a, E_b, U_c 再包含 E_c 或 U_b 之一的公理系是完备的.

因为没有公理 U_a，所考察的集合 G 中任意两个元素 b 与 c 的乘积可能有许多值. 因此，我们约定用符号 bc 表示这些值的全体. 如果元素 a 是 b 乘以 c 所得的乘积之一，我们就约定用符号

$$bc \ni a$$

来表示. 如果 A_1 和 A_2 是 G 的任意两个子集，那末就用 A_1A_2 表示 G 中所有由 A_1 的每一元素乘以 A_2 的每一个元素而得到的结果所组成的集合. 显然

(α) 若 $A_1 \supseteq A_2, A_3 \supseteq A_4$，则 $A_1A_3 \supseteq A_2A_4$.

其次，由公理 U_c 得

(β) 若 $aB \ni d, ac \ni d$，则 $B \ni c$.

由(β)得出，如果 $ab \supseteq ac$，则 $b=c$.

现在来证明引理. 取任意元素 d. 我们证明，存在这样的元素 e，使得 $de \ni d$. 如果我们的公理系包含 U_c 的话，以上所说是显然的. 如果公理系包含 E_b，那末由 E_b 可知，存在一个 e，使得 $ed \ni d$；再根据(α)，得 $ded \supseteq dd$，于是由 U_b，得 $de \ni d$.

如果 f 是另外一个元素，那末 $def \supseteq df$. 由(β)得，$ef \ni f$. 再根据 E_b，存在元素 g，使得 $gf \ni d$，从而

$$gfe \supseteq de \ni d.$$

于是由(β)得出，$fe \ni f$，即元素 e 对于 G 的所有元素来说，既是左单位元又是右单位元. 再由公理 U_c 可以推得元素 e 的唯一性.

现在设 $ee\ni h$,. 由 $eh\ni h$ 再根据 U_c, 我们有 $h=e$, 即 $ee=e$. 其次, 如果 $ef\ni k$, 那末 $ef=eef\ni ek$. 于是由(β)的推论得 $k=f$, 即对于一切 f 都有 $ef=f$. 然而我们暂时还不能用等式来代替包含关系 $fe\ni f$. 由公理 E_b, 存在元素 f^{-1}, 使得 $f^{-1}f=e$. 于是 $f^{-1}ff^{-1}\ni ef^{-1}=f^{-1}$. 又因为 $f^{-1}e\ni f^{-1}$, 所以由(β)得

$$ff^{-1}\ni e.$$

因此, 元素 f^{-1} 是由元素 f 唯一确定的. 用 f^{-1} 代替 f, 我们有

$$f^{-1}(f^{-1})^{-1}\ni e.$$

又因为 $f^{-1}f\ni e$, 所以由(β)得 $(f^{-1})^{-1}=f$.

现在设 $ff^{-1}\ni l$. 则 $ff^{-1}l^{-1}\supseteq ll^{-1}\ni e$. 再由($\beta$), $ff^{-1}\ni e$, 从而得出

$$f^{-1}l^{-1}\ni f^{-1}.$$

于是由公理 U_c, 我们有

$$l^{-1}=e,\quad l^{-1}l=el.$$

再由 $l^{-1}l\ni e=ee$, 根据(β) 推出 $l=e$, 即对于一切 f 都有 $ff^{-1}=e$. 以 f^{-1} 代替 f, 我们有

$$f^{-1}f=e.$$

现在设 $bc\in a$. 那末

$$c=ec=b^{-1}bc\ni b^{-1}a.$$

于是根据 U_c, 元素 a 由元素 b 和 c 唯一确定, 即公理 U_a 成立. 由 §3 可知, 单位元和逆元存在. 现在就可以认为引理 2 已经证毕.

利用左除与右除的对称性, 我们有以下引理.

引理 3 任何一个包含 A, E_a, E_c, U_b 再包含 E_b 或 U_c 之一的公理系是完备的.

现在可以毫无困难地证明, 性质 1—4 对于公理系的完备性来说是充分的. 事实上, 任何一个具有性质 1—4 的公理系至少应该包含下列五个子系之一:

$$A,\begin{pmatrix} & E_b & E_c \\ U_a & & \end{pmatrix};\ A,\begin{pmatrix} E_a & E_b & E_c \\ & U_b & \end{pmatrix};\ A,\begin{pmatrix} E_a & E_b & E_c \\ & & U_c \end{pmatrix};$$

$$A,\begin{pmatrix} E_a & E_b & \\ & U_b & U_c \end{pmatrix};\ A,\begin{pmatrix} E_a & & E_c \\ & U_b & U_c \end{pmatrix}.$$

由引理 1—3 容易推出，这五个子系中每一个都是完备的. 同时我们也看到，这些公理系都是最小完备系. 因此就证明了，在群定义的七条公理中，可以组成五个不同的最小完备系. 自然，最有趣的是第一个公理系，它告诉我们，乘积的存在是乘积的唯一性和两侧商的存在以及结合律的必然结果.

关于处理这个问题的另一种方法，可以参看 P. Lorenzen [1].

§4. 群的例子

这一节里我们将要举出几个最简单的群的例子，这些例子下面经常要引用到，在大多数情形下，验证群的定义中各项要求是否满足，这项工作多半留给读者去做.

1. 全体整数对加法运算组成一个群——整数加法群. 这是一个阿贝尔群，在它里面零这个数起着单位元素的作用. 除零外，这个群里所有元素都有无限阶，也就是说，这个群是一个无扭群.

2. 用同样的办法可以得出全体有理数的加法群、全体实数和全体复数的加法群.

3. 全体偶数对加法组成一个群. 这个偶数加法群和整数加法群(例 1)同构. 事实上，将每个偶数$2k$映成整数 k 的映射是一个同构映射. 某一整数 n 的倍数的全体，也对加法组成一个群. 奇数的集合对于加法运算已经不能成为一个群，因为这个运算会使我们超出集合的范围. 全体非负整数的集合对于加法也不能组成一个群，因为在这个集合里逆运算——减法——不能无限制地进行.

4. 整数对于乘法不能组成一个群，因为逆运算——除法——不能经常进行. 对于乘法来说，全体有理数也不能组成一个群，因为不能用零去除. 全体不等于零的有理数对乘法来说组成一个群——有理数乘法群. 这个群的单位元素就是1. 这个群里面的数-1的阶是2，所有其余异于单位元的数是无限阶的.

5. 也可以说正(异于零)有理数乘法群. 这个群能以下述方式同态地映射到整数加法群上：任何正有理数α能写成形式

$$\alpha=2^n\alpha',$$

此处，数α'的分子和分母与数2互素，而整数n大于、等于或小于零. 映射$\alpha\to n$就是所要求的同态映射. 注意，对乘法来说负有理数已经不组成一个群.

6. 全体异于零的(或全体正的)实数，与全体异于零的复数对于乘法也同样各组成一个群. 如在§2已指出的，应记得正实数乘法群和全体实数加法群同构.

7. 数1和-1对于数的乘法运算组成一个群——二阶有限群. 如在§2曾提到过，整数加法群可同态映射到这个群上. 全体非零实数乘法群也能同态映射到它上——规定所有正数对应数1，所有负数对应数-1就行了.

8. 1的n次根的全体复数，对于乘法组成一个n阶有限群. 这就证明了任意阶的有限群存在. 在$n=2$时便得到前例中的群. 要记住，1的所有n次根，都是其中一个根的幂，即所谓1的n次本原根的幂.

9. 1的任何次根的全体复数，对乘法也组成一个群；这是全体单位根群. 它有无限多元素，然而所有元素都是有限阶的，是个周期群.

10. 绝对值等于1的全体复数对于乘法组成一个群. 这个群与圆周旋转群同构. 让我们考察圆周以反时针方向绕其中心的全

体旋转的集合. 角度 2π的旋转认为与角度零的旋转相重合，并且一般地，角度为 2π 倍数的彼此不同的任何两个旋转我们认为同一的. 用以下方式在这个旋转的集合中定义群的运算：两个旋转的和认为是它们接连施行的结果；显然，角度为 α 与 β 的旋转之和，在 $\alpha+\beta<2\pi$ 时，是角度为 $\alpha+\beta$ 的旋转；在 $\alpha+\beta\geqslant 2\pi$ 时，是角度为 $\alpha+\beta-2\pi$ 的旋转. 易于检验这里得到的是个群. 这个群到上述绝对值等于 1 的复数乘法群上的同构对应，只要在角度为 α 的旋转和以 α 为辐角的复数间建立对应就可得到.

上面所考察的群都是交换的. 现在我们来看非交换群的例子.

11. n 个符号的全体置换，把在 § 1 里所定义的置换乘法作为群的运算，组成一个群 S_n—— n 次对称群. 这是 $n!$ 阶有限群. 在 $n\geqslant 3$，它是非交换的. 事实上，在 § 1 证明过置换乘法的结合律，并且表明恒等置换起着单位元素的作用；置换

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

的逆元素是置换

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

12. 在高等代数教程[1]已知，在 $n>1$ 时，全体 n 次置换可分为奇与偶两类，并且每类各有 $\frac{1}{2}n!$ 个. 各种可能的定义中我们讲这样的一种定义：如果置换可分解为偶数个对换之积，则称为偶置换；而在相反的情形，则称为奇置换. 由此推出，两个偶置换的

1) 例如，参看库洛什(А. Г. Курош)著“高等代数教程”，(有中译本，柯召译，高等教育出版社，1955 年 8 月新一版)第六版，§ 3，在那里还能找到在下面要屡次利用的分解置换为对换的积和分解置换为相互独立的循环置换的积.

积是偶置换．因为恒等置换显然是偶的，偶置换的逆置换也是偶的，所以我们得到用 A_n 表示的全体 n 次偶置换群；它叫做 n 次交错群．这是一个 $\frac{1}{2}n!$ 阶有限群，在 $n\geqslant 4$，是非交换的．

n 次奇置换已经不能组成一个群，因为两个奇置换的积已是偶置换．

现在易于检验，存在将群 S_n 映到例 7 所述二阶群上的同态映射：每个偶置换应规定对应数 1，每个奇置换应规定对应数 -1．

13．取某个集合 M，并考虑它到其自身上的所有可能的相互单值映射．因为接续施行两个这样的映射重新给出集合 M 到其自身上的一个相互单值映射，因而在这映射集合中接续施行就是我们所要的运算．它的结合律在 §1 曾证明过，恒等映射是单位元素，对所有的映射都存在逆映射．因此我们得到集合 M 到其自身上的全体相互单值映射群 S_M．如设集合 M 是有限的，且由 n 个元素组成，则我们的群成为 n 次对称群．显然，假若集合 M 和 M' 有同一的势，则群 S_M 和群 $S_{M'}$ 同构．

这个例子很重要，因为在群的应用中常常出现所谓变换群，这就是某个集合 M 到其自身上的相互单值的映射群，而以接续施行映射作为这个群的乘法．诚然，通常我们不考察全体这样的映射，而仅考察某些具有给定附加性质 α 的映射，或简称为 α- 变换．为要集合 M 的所有 α- 变换组成一个群，显然，满足下两条件就够了：

1）两个 α- 变换的积必须具有性质 α；

2）α- 变换的逆映射必须具有性质 α．

这个注意，在考察以后的例子时将用到，那些例子的每一个都是某个集合 M 在某性质 α 条件下的全体 α- 变换群．特别在这些例子中，乘法永远被了解为接续施行映射．

14. 取势为$\mathfrak{M}$的无限集合，并仅仅考察这个集合到其自身上的这样一些相互单值的映射，这种映射的每一个，实际上只变动有限个符号，虽然这个数目也可能任意的大. 这些映射组成一个势为$\mathfrak{M}$的周期群，称做势为$\mathfrak{M}$的对称群. 因为在此处所考察的映射能够采用上面给出过的置换的奇偶性的定义(为此，只要考察实际上变动了的符号)，由类似的方法我们得到势为$\mathfrak{M}$的交错群.

15. 让我们考察实数域上（或一般地任意域上）n维矢量空间. 这个空间的非退化线性变换对乘法组成一个群，当$n\geqslant 2$时是非交换群；从高等代数教程知道，在非退化线性变换和n阶非退化方阵之间存在相互单值对应，变换的积对应于相应方阵的积. 因此，我们的群和n阶非退化方阵乘法群同构. 注意，每个这样的群同态地映射到异于零的实数乘法群上：规定每个方阵对应它的行列式，并考虑到方阵乘积的行列式等于其因子行列式的乘积，就可得到证明.

16. 三维欧氏空间的运动组成一个群. 保持给定点不动的那种运动，即是围绕这不动点的旋转，也是如此.

17. 欧氏空间的这些旋转，使给定立方体以其中心为不动点到其自身上的映射，组成一个群. 这个立方体的旋转群是有限阶的，因为它的元素相互单值地对应立方体顶点集合的某个置换，并且易于检验，它是非交换群. 用类似的方法，我们同样可定义其他的正多面体的旋转群.

第二章 子　群

§5. 子　群

如果群G的子集合H对于群G中的运算也构成一个群，那末H称为G的*子群*.

为了断定群G的(非空) 子集合H究竟是不是群G的子群,只要验证下列两点就够了:

1) 在H中是否包含H的任何两个元素的积;

2) 在H中，与其每一元素本身一起，是否还含有它的逆元素.

事实上,因为结合律在群G中成立，于是对H的元素也成立;而集合H是非空的,同时又由于性质 2)和 1)，于是群G的单位元素也属于H.

在有限群及一般的周期群的情形，验算性质 2) 实是多余的.实际上,如果n阶的元素a属于H,那末，由于性质 1)，在H中必然包含元素a的所有正指数幂,因此,也包含元素a^{n-1}，即a的逆元素. 整数加法群及其正整数部分集合这个例子，说明了在一般情形下有必要来验证性质 2).

我们着重指出,在子群的定义里,要求群G的子集合对定义于G中的运算成为群,这子集合才算是子群,而不能说群G的凡是自成其为群的任何子集合都是子群. 例如，正有理数的集合对乘法构成一个群，且作为一个子集合包含在由所有有理数所组成的加法群内,但当然不是这个群的子群.

“H是G的子群”这个关系是可传递的：如果H是G的子群，而G又是$\bar{G}$的子群,则H也是$\bar{G}$的子群.

群G中，由一个元素 1 所组成的子集合，显然是这个群的子

群. 这个子群称为群 G 的单位子群，并记作 E. 在另一方面，群 G 本身也是它自己的子群. 任何不等于整个群的子群都称为这个群的真子群.

在 §4 里所举出的群中，有许多是在同一节中所述其他群的子群. 例如，偶数加法群是全体整数加法群的子群，而后者又是全体有理数加法群的子群. 所有这些群，和一切由数所组成的加法群一样，都是复数加法群的子群. 正有理数乘法群和由 1 与 -1 两个数所组成的乘法群，是由所有不等于零的有理数所组成的乘法群的子群. n 次交错群是同次对称群的子群. 由某一集合 M 的所有 α- 变换所组成的群，其中包括在 §4 例 14—17 中所讨论的群，都是由集合 M 到其本身的一切相互单值映射所组成的群 S_M 的子群.

上一段中所引述的第一个例子表明，一个群的真子群可能和这个群本身同构，——在 §4 中已经建立了整数加法群和偶数加法群间的同构. 不难理解，没有一个有限群能和它的真子群同构.

在群 G 到 $\bar{G}$ 上的一个同态(特别是同构)映射 φ 之下，群 G 的子群 A 被映到群 $\bar{G}$ 的一个子集合 $\bar{A}$ 上. 映射 φ 是 A 的一个同态(特别是同构)映射. 因此，根据 §3 中所证，集合 $\bar{A}$ 对在 $\bar{G}$ 中定义的运算构成一个群，也就是说，它是这个群的一个子群. 我们说，群 G 的这个同态映射产生了 G 中所有子群的同态映射.

如果已经给定两个群 G 和 G'，且群 G' 和群 G 的一个子群 H 同构，那末就说群 G' 可同构地映入群 G 内，或者说群 G' 可嵌入群 G 内. 在 H 和 G 相重合这一特殊情形下，就说 G' 可同构地映到群 G 上. 然而这里必须注意一点，即群 G' 一般说来可由多种不同的方式同构地映到 H 上. 除此以外，子群 H 也不一定是群 G 中唯一和群 G' 同构的子群；群 G 中所有和 G' 同构的子群彼此同构，但他们是群 G 中互不相同的子集合，因此在群 G 内部对这些子群必须予

以区别. 如果将群 G' 作任何一个同构映射,使它映到群 G 的与它同构的一个子群上,这样的映射只能给出将群 G' 嵌入群 G 中的各种可能方法中的一种.

现在让我们取 n 次对称群 S_n 作为例子来考察这个问题. 如果 i 是 n 个(要进行置换的)符号 $1,2,\cdots,n$ 中的一个, 则群 S_n 中所有使 i 不动的置换组成 S_n 的一个子群. 这个子群和 S_{n-1},即 $n-1$ 次对称群同构. 因此可以说, $n-1$ 次对称群可嵌入 n 次对称群内;同时还可以看出,群 S_n 包含 n 个彼此互异的与群 S_{n-1} 同构的子群.

如果已知两个群 A 和 B, 且其中每一个群与另一群的某一个真子群同构, 从这个事实并不能像我们可能预想的那样, 推出这两个群本身彼此同构. 从这里只能推出每一个群都和自己一个真子群同构,而这一点对我们来说已经不是什么想像不到的事了.事实上,若

$$A\simeq B'\subset B$$

且若在群 B 同构地映入群 A 时,子群 B' 映到子群 A'',则 A'' 就是和 A 本身同构的子群.

下面的定理表明,有限对称群实际上穷尽了所有有限群.

Cayley **定理** 任何一个 n 阶有限群都和 n 次对称群的一个子群同构.

事实上, 假设群 G 有阶数 n, 且这个群的元素可按一定次序记作

$$a_1, a_2\cdots, a_n. \tag{1}$$

如果 b 是群 G 内任意一个元素, 则所有乘积 $a_ib=a_{\beta_i}(i=1,2,\cdots,n)$ 彼此不同,也就是说,元素系

$$a_{\beta_1}, a_{\beta_2}, \cdots, a_{\beta n} \tag{2}$$

仍又包含群 G 中所有元素, 而与(1)不同之处仅在于元素的次序.

现在可使置换

$$\begin{pmatrix}1 & 2 & \cdots & n\\ \beta_1 & \beta_2 & \cdots & \beta_n\end{pmatrix} \tag{3}$$

与元素 b 相对应. 对群 G 中每一个元素，用这一方法可使一个完全确定的 n 次置换与之相对应. 和不同元素相对应的置换也彼此不同，因为由 $a_1b=a_1b'$ 即可得出 $b=b'$. 现在让我们求出和乘积 bc 相对应的置换，这里 c 是群 G 中一个元素. 如果和元素 c 对应的置换是

$$\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_n\\ \gamma_1 & \gamma_2 & \cdots & \gamma_n\end{pmatrix}, \tag{4}$$

也就是说，如果 $a_{\beta_i}c=a_{\gamma_i}$，则由

$$a_i(bc)=a_{\beta_i}c=a_{\gamma_i}$$

可以看出，和元素 bc 对应的置换是

$$\begin{pmatrix}1 & 2 & \cdots & n\\ \gamma_1 & \gamma_2 & \cdots & \gamma_n\end{pmatrix}.$$

这个置换显然是置换(3)乘上置换(4)的积. 这样就证明了群 G 可以同构地映入群 S_n. 群 S_n 中和 G 对应的子群显然具有下述性质，这个子群的阶数等于置换中符号的个数；除单位置换以外，这个子群中的任何置换实际变动了每一个符号. 对称群的这样一种子群称为*正则子群*.

由 Cayley 定理和一个*有限群只能具有限多个子群*这样一个明显的论断，可以推出，*阶数 n 为一定，但互不同构的有限群只有有限多个*. 因此，所有互不同构的有限群的集合，是可数多个有限集合的和，因而是一个可数集合.

Cayley 定理可推广于无限群：任何一个势为 $\mathfrak{M}$ 的群，都和一个势为 $\mathfrak{M}$ 的集合到其本身上所有相互单值映射的群 $S_{\mathfrak{m}}$ 中一个子群同构(参看 §4，例 13). 事实上，上面的证明在这里完全适用，只

有一项断言，即用元素 b 右乘群中所有元素后能仍又给出这个群中所有元素这一点，还需要作一些补充的考虑；然而这一点可由左侧商存在这一公理立即推出.

子群的概念是群论中一个基本概念. 群论的全部内容都在或大或小的程度上和子群的问题有关：如关于具有特别性质的子群的存在的问题，关于能嵌入一个已知群中的群的问题，关于决定一个群中各个子群的相互位置的某些性质的问题，以及根据一个群的子群来构成这个群的方法等问题就是. 某些特殊类型的群的区分也主要是和子群的概念有关.

§6. 生成系·循环群

群 G 中任意两个子群 H 和 F 的交不可能是一个空集合，因为群 G 中任何一个子群都包含元素 1. 这个交实际上是群 G 的一个子群：如果 D 是子群 H 和 F 的交，$D=H\cap F$，且设元素 a 和 b 属于 D，则这两个元素的乘积和他们的逆元既包含在 H 内，又包含在 F 内，因而也同样属于 D.

如果在群 G 中所给出的不是两个，而是任意有限多个，或者甚至是无限多个子群，则所有这些子群的交中任意两个元素的乘积包含在这些子群中的每一个内，因而包含在他们的交内. 对于逆元来说，这个事实也是正确的. 因此，群 G 中任意一组子群的交是这个群的子群. 这样，群 G 中所有子群的交显然就是单位子群 E.

假设 M 是群 G 中任意一个非空子集合. 群 G 中包含 M 中所有元素的一切子群——群 G 本身当然是这样的子群之一——的交，称为由集合 M 所生成子群，并用记号 $\{M\}$ 来表示. 这个子群显然包含在群 G 中任何一个含有整个集合 M 的子群之内.

如果子集合 M 是由一个单独的元素 a 所组成的，则由它所生成的子群 $\{a\}$ 称为元素 a 的循环子群. 元素 a 的各次幂当然属于

循环子群$\{a\}$；但是元素a^n和a^m的乘积等于a^{n+m}，而元素a^n的逆元即是a^{-n}(参看 §3)，所以这些幂本身组成一个子群，由此可知*循环子群$\{a\}$由元素a的所有的幂所组成*．这个事实表明，如果元素a是一个无限阶元素，则循环子群$\{a\}$是一个可数子群，而在元素a的阶数为有限时，则$\{a\}$为有限群．在后一种情形下，子群$\{a\}$的阶即等于元素a的阶．

和本身的一个循环子群相重合的群，也就是说，由本身的一个元素的幂所组成的群，称为*循环群*；这样的元素，它的幂组成这个循环群的，称为这个群的*生成元*．很显然，任何循环群都是交换群．

整数加法群是无限循环群的一个例子——它的生成元是整数1；而由n次单位根($n=1, 2, \cdots$)所组成的乘法群则是有限循环群的例子．下面的定理表明，这些例子实际上已经穷举了所有的循环群．

所有无限循环群彼此同构；具有给定阶数n的所有有限循环群也彼此同构．

事实上，如果取任何一个元素a^k，使整数k和它相对应，则一个以元素a为生成元的无限循环群即可相互单值地映射到整数加法群上；至于这个映射之为同构映射，则可由这样一个事实看出，即元素a的幂相乘时，他们的指数相加．用同样方法可以得出任何n阶循环群到n次单位根群上的同构映射．

有了这个定理以后，就可以直接谈论*无限循环群*，或*n阶循环群*．

在一个循环群中，任何一个子群都是循环群．

事实上，假设$G=\{a\}$是一个以元素a为生成元的无限或有限n阶循环群，而H则为G中不等于E的子群．再假定包含在H中的元素a的最低正幂为a^k．这时就有$\{a^k\}\subseteq H$．假定H同时还包

含一个元素 a^l, $l\neq 0$, 且 l 不能被 k 所整除. 在这时, 如果 $(k, l)=d$, $d>0$, 是 k 和 l 的最大公约数, 就有两个这样的整数 u 和 v 存在, 使得 $ku+lv=d$. 因此 H 应包含元素

$$(a^k)^u(a^l)^v=a^d.$$

但因为 $d<k$, 所以我们得出的结果和元素 a^k 的选择相矛盾. 因此, $H=\{a^k\}$.

在以元素 a 为生成元的无限循环群中, 元素 a^{-1} 同样也可以取作生成元; 而由元素 a 的任何其他幂所生成的循环子群则不能等于整个群. 在 n 阶循环群 $\{a\}$ 中, 元素 a^k, $0\leqslant k<n$, 能被取作生成元的充分必要条件是 k 和 n 互素.

事实上, 如果 $(k, n)=1$, 就有两个这样的整数 u 和 v 存在, 使得

$$ku+nv=1.$$

在这时,

$$(a^k)^u=a^{1-nv}=a\cdot a^{-nv}=a.$$

另一方面, 如果对于某一整数 k 有 $(a^k)^s=a$, 则两个指数的差 $ks-1$ 应该能被 n 所整除(参看 §3):

$$ks-1=nq,$$

由此得出

$$ks-nq=1,$$

也就是说, $(k, n)=1$.

现在重新假定 M 是群 G 中一个任意的子集合. 和循环群的情形一样, 容易指出怎样用集合 M 中的元素来表示子群 $\{M\}$ 的元素的规则来. 子群 $\{M\}$ 应包含 M 中所有元素的正幂和负幂; 因而包含按任意次序取出的任意有限多个这样的幂的乘积. 但是群 G 中所有能够表成 M 中有限多个元素的幂积的元素 (虽然表示方法有许多种), 显然组成一个包含 M 的所有元素的子群. 这样就证明

了，由集合M所生成的子群，是由群G中所有等于集合M中有限多个元素幂积的元素所组成的.

就其特例而言，如果已知群G中有一组子群，而M是这些子群的集合和，也就是说，如果M是这样一个集合，它由群G中至少在一个给定的子群中出现的元素所组成，则$\{M\}$就是群G中包含所有这些子群的最小子群. 这个子群$\{M\}$称为由这些已给子群所生成的子群. 如果已知的子群为A_α，其中α遍历某个足标集合N，则$\{M\}$可记作$\{A_\alpha\}$，$\alpha\in N$；在特例，如果所给的只有两个子群A和B，则子群$\{M\}$可用记号$\{A, B\}$表示，余类推. 由以上所述可知，群G中一组已给子群所生成的子群，由G中所有这样的一些元素所组成，它们等于取自这些子群的有限多个元素的乘积.

如果由群G中一个子集合M所生成的子群$\{M\}$和群G本身重合，集合M就称为这个群的生成元素系，或简称作生成系. 任何一个群都有生成系——只要取由群G中所有元素所组成的集合，或由1以外所有元素所组成的集合作为M就行了. 由上面所述可知，要使集合M是群G的生成系，其充分必要条件是：G中任何一个元素至少可用一种方式表成M中有限多个元素幂乘积的形式.

假设

$$G=\{M\};$$

如果生成系M的任何子系都不是G的生成系，M就称为G的既约生成系.

例1. 任何循环群都有一个生成系，即由这个群的一个生成元素所组成的生成系. 反之，任何一个具有单独元生成系的群都是循环群. 可注意的是：在一个循环群中通常也可以找出由一个以上的元素所组成的既约生成系来，例如整数2和3就组成整数加法群的一个既约生成系.

2. 在§4曾提到过，所有n次置换都是对换之积. 由此推出，

包含在这个群中的所有对换的集合是 n 次对称群的一个生成系.

n 次对称群同样也可由两个生成元

$$a=(1,2),$$
$$b=(1,2\cdots,n)$$

所生成. 事实上

$$b^{-k}ab^{k}=(k+1,k+2),k\leqslant n-2.$$

如果 $i<j-1$, 则有

$$(j,j-1)\cdots(i+2,i+1)(i,i+1)(i+1,i+2)\cdots(j-1,j)=(i,j),$$

也就是说,子群 $\{a,b\}$ 包含所有对换, 因而和整个对称群重合.

3. 有理数

$$1,\frac{1}{2},\ \frac{1}{6},\ \frac{1}{24},\ \cdots\frac{1}{n!},\ \cdots$$

组成有理数加法群 R 的一个生成系. 不难看出,这个集合的任何一个无限子集合都是 R 的生成系. 除此以外,还可以证明,*有理数加法群 R 没有任何既约生成系*. 事实上,假定 M 是 R 的一个生成系,而 a 是 M 中任意一个元素. 我们用 H 来表示除 a 外 M 中所有其他元素的集合 M' 所生成的子群;集合 M' 不可能是空集合, 倘若不然, 所有的有理数都将是 a 的倍数, 而这是不可能的. 如果 b 是 M' 中任意一个元素,则由有理数的性质可知, 可以找到这样一个不等于零的整数 k 使 ka 是有理数 b 的倍数, 因而包含在子群 H 中. 有理数 $\frac{1}{k}a$ 属于群 R, 因而可以表作 M 中某些有理数的倍数的有限和,也就是说表成

$$\frac{1}{k}a=sa+h$$

这种形式,其中 s 是一个整数, 可能等于零;而 h 则为子群 H 中的元素,由此得出

$$a=s(ka)+kh,$$

也就是说，a 包含在H里，因而 $H=R$，因此集合 M' 是群R的生成系.

4. 正有理数乘法群有一个既约生成系，这个生成系由所有素数组成.

如果群G有一个由有限多个元素组成的生成系，G就称为*具有限生成系的群*。很显然，所有有限群和所有循环群都是具有限生成系的群. 无限循环群的例子表明，不能由生成元的个数为有限这一事实推出群本身为有限群.

在一个具有限生成系的群中，任何一个生成系都包含这样一个有限子集合，它是这个群的既约生成系.

因为任何一个有限生成系都可去掉其中多余的元素而使之成为既约生成系，所以只要证明，在上述的条件下，任何一个无限生成系都包含一个同样可以作为所论群的生成系的有限子集合即可. 假设G是以 $a_1, a_2, \cdots, a_n$ 为生成元的群

$$G=\{a_1, a_2, \cdots, a_n\},$$

而M是这个群的另一生成系. 任何一个元素 a_i, $i=1,2,\cdots,n$, 都可表作 M 中有限多元素的幂的乘积. 我们可以对每一个元素 a_i $(i=1,2,\cdots,n)$ 挑选出一个这样的表示式，并将出现在这些表示式中的M的元素归集在一起，而得出M的一个有限子集合 M'. 由 M' 生成的子群$\{M'\}$包含所有元素$a_1, a_2, \cdots, a_n$，因而与G重合. 可注意的是，在一个具有限生成系的群中，不同的既约生成系一般说来可以包含不同数目的元素(参看例 1).

一个具有限生成系的群的任何同态像本身也是一个具有限生成系的群.

事实上，如果

$$G=\{a_1, a_2, \cdots, a_n\},$$

而同态对应φ将群G映到群 $\bar{G}$ 上，则元素

$$a_1\varphi, a_2\varphi, \cdots, a_n\varphi \tag{1}$$

组成 $\bar{G}$ 的一个生成系. 事实上, 如果 $\bar{a}$ 是群 $\bar{G}$ 中任意一个元素, 而 a 是它在群 G 中的一个原像, 则 $\bar{a}$ 就能够按照用元素 $a_2, a_2, \cdots, a_n$ 的幂来表示 a 的方式, 用元素(1)的幂表示出来. 当然, 元素(1)中可能有某些元素彼此重合, 也就是说, 我们所得出的(1)是群 $\bar{G}$ 的一个有重复的生成系. 此重复的元素是可以去掉的, 然而, 将来我们也可考虑含有重复元素的生成系.

任何具有限生成系的无限群, 都是可数群。

事实上, 如果元素 $a_1, a_2, \cdots, a_n$ 是群 G 的生成元素, 则群中任何元素都能表成乘积

$$a_{i_1}^{\alpha_1}a_{i_2}^{\alpha_2}\cdots a_{i_s}^{\alpha_s}$$

的形式(一般说来, 表示方式有许多种); 任何一个 i_k 都是整数 1, 2, ⋯, n 中的一个, 并且当 $k \neq l$ 时, 可能有 $i_k = i_l$. 各个指数的绝对值的和

$$h = |\alpha_1| + |\alpha_2| + \cdots + |\alpha_s|$$

称为这个乘积的长度. 不难看出, 当长度 h 为一定时, 生成元素 $a_1, a_2, \cdots, a_n$ 的幂积只有有限多个. 因此所有这些元素的幂积的集合是可数多个有限集合的和, 也就是说, 是一个可数集合, 因而群 G 不会比一个可数群更大一些.

本节中的例 3 和例 4 表明, 不具有限生成系的可数群是存在的. 因此具有限生成系的群实际上是位于有限群和可数群之间的一类群.

就一个具有限生成系的群说, 它的任何一个子群当然不会比一个可数群再大. 然而在第九章中我们将会看到具有限生成系的群的例子, 它的某些子群却不具有限生成系. 具有限生成系的群将在第十章中专门来讨论.

还可以指出, 用与以上所述完全相同的方法可以证明; 如果群

G有一个势为$\mathfrak{M}$的生成系(没有重复出现的元素)，则这个群本身的势也是$\mathfrak{M}$.

§7. 递增群列

假定在群G中已经给出了一组子群，并且这些子群构成一个递增序列

$$A_1, A_2, \cdots, A_n, \cdots,$$

也就是说，给出了这样一组子群，他们之中任何一个子群A_n包含在子群A_{n+1}里，$A_n \subseteq A_{n+1}$，$n=1, 2, \cdots$. 这个递增子群列的并集B是群G的一个子群，因而是由子群A_n所生成的子群.

事实上，集合B中任何一个元素b必定包含在某一个子群A_n内(一般地，包含在所有A_k里，$k \geqslant n$). 这时元素b^{-1}也包含在A_n内，因而包含在B内. 如果从B中已经取出了两个元素b_1和b_2，并且这两个元素分别包含在子群A_n和A_k内，我们可以假设$n \leqslant k$. 这时元素b_1和b_2同时包含在子群A_k内，这样一来乘积b_1b_2也包含在这个子群内，因而包含在B内. 这就证明了集合B是群G的子群.

除按自然数列序型排列的可数子群列外，也可以讨论任意一组具有下述性质的子群A_α，即出现在这一组子群里的任意两个子群A_α和A_β中，必定有一个子群包含在另一个之内[1]. 这些群的并集也是群G的一个子群；只要将上节中所作的证明逐字重复说一遍就可以证明这一点。

本书以下各章节中要多次用到下面的定理:

若在群G中已经给出了一个子集合M和一个子群A，且二者

1) 如果将子群A_α, A_β中包含在另一子群内的那个群看作先行元素，这些子群就组成一个有序集合. 这个有序集合当然不一定是良序的.

的交为子集合D，则在G中至少存在一个包含A的子群，它与M的交为D，并且它不包含在任何一个具有这两项性质的子群内。

假定群G的元素是良序的：

$$1=a_0, a_1, \cdots, a_\alpha, \cdots$$

命$A_1=A$. 假设对所有的$\beta<\alpha$，在G中已经选出了一组构成一个递增序列的子群A_β，且有这样的性质，即他们之中每一个子群和M的交都是D. 设B_α是由子群$A_\beta(\beta<\alpha)$所组成的递增序列的并集. 如果子群$\{B_\alpha, a_\alpha\}$与M的交等于D，那末我们就取子群$\{B_\alpha, a_\alpha\}$作为A_α；而在相反的情况下，则取B_α作为子群A_α. 由所有子群A_α所组成的递增序列的并集$\bar{A}$，就是所求的子群：$\bar{A}$和M的交显然是D；如果元素a_γ在群$\bar{A}$之外，那末子群$\{\bar{A}, a_\gamma\}$与M的交就不等于D，因为我们已经有$\{B_\gamma, a_\gamma\}\cap M\neq D$.

由这个定理可得出一个特例：如果群G中有与M不相交的子群存在，那末在这些子群中至少有一个极大的.

群G中递增子群列

$$A_1\subseteq A_2\subseteq\cdots\subseteq A_n\subseteq\cdots$$

的并集可能和这个群本身重合. 现在让我们举出几个这样的例子：

1. 有理数加法群R是递增循环子群列：

$$\{1\}\subset\left\{\frac{1}{2}\right\}\subset\left\{\frac{1}{6}\right\}\subset\cdots\subset\left\{\frac{1}{n!}\right\}\subset\cdots$$

的并集.

2. 设G为正有理数乘法群，而

$$p_1, p_2, \cdots, p_n, \cdots$$

则为按增大次序排列的全部素数. 如果命

$$A_n=\{p_1, p_2, \cdots, p_n\},$$

这里A_n是这样的全体有理数，其既约分数表示式的分子和分母中，只有$p_1, p_2, \cdots, p_n$等素数出现，则群G就是递增子群列A_n($n=$

1, 2, …)的并集.

3. 设 S_ω 是可数对称群，就是说，S_ω 是由可数集合 $x_1, x_2, \cdots, x_n \cdots$ 到其本身上的一切相互单值映射所组成的群，其中每一个映射实际上只变动有限多个符号. 在这个群中，使符号

$$x_{n+1}, x_{n+2}, \cdots$$

都不变动的映射组成子群 S_n，这 S_n 显然和 n 次对称群同构. 群 S_ω 与子群 $S_n, n=1, 2, \cdots$, 的并集重合.

另一方面，下面的定理成立：

一个具有限生成系的群，不能与它的递增真子群序列的并集重合。

假设群 G 有一个有限生成系

$$G=\{a_1, a_2, \cdots, a_n\},$$

并且假设它和它的一个递增真子群序列

$$H_1 \subset H_2 \subset \cdots \subset H_k \subset \cdots$$

的并集重合.

每一个元素 $a_i, i=1, 2, \cdots, n$, 或者更一般地，G 中任何一个元素，一定属于某一个子群 H_{k_i}，因而属于所有的子群 $H_k, k \geqslant k_i$. 如果

$$l=\max(k_1, k_2, \cdots k_n),$$

则所有元素 $a_1, a_2, \cdots, a_n$ 都包含在 H_l 里；因而由他们生成的子群不能和 G 重合.

如果在具有限生成系的群中，所给的是按任意方式排列的递增真子群列，这个证明也仍然适用.

由可数子群组成的递增序列的并集，或就其特例而言，由具有限生成系的子群所组成递增序列的并集，当然是一个可数子群. 反之，任何一个可数群都是一个由具有限生成系的子群所组成的递增序列的并集。

事实上，假设可数群G的元素按某一任意方式编号之后是

$$g_1, g_2, \cdots, g_n, \cdots.$$

如果命H_n为群G中由元素$g_1, g_2, \cdots, g_n$生成的子群

$$H_n=\{g_1, g_2, \cdots, g_n\},$$

所有子群H_n都是具有限生成系的群，一个包含在另一个内(在这里可能出现等式$H_n=H_{n+1}$的情形)，而群G为这一递增子群列的并集.

现在我们要说明一项构成法. 这一构成法有时使我们能够考察这样的递增序列：构成这递增序列的，是一些并非预先就包含在某个总的群内的群.

假设已经给定了一组群

$$G_1, G_2, \cdots, G_n, \cdots \tag{1}$$

且对每一n，都给定了一个把群G_n映入群G_{n+1}的同构映射φ_n(即映到后者的某一个子群上)，

$$g_n\varphi_n=g_{n+1}, \quad g_n\in G_n; \quad g_{n+1}\in G_{n+1}. \tag{2}$$

有了群(1)和同构映射(2)之后，可以按下述方式作出一个新的完全确定的群$\bar{G}$来.

我们称任何一个有下述性质的元素列

$$\gamma=g_k, \quad g_{k+1}, \cdots, g_n, \cdots \tag{3}$$

为一个元素络：1) $k\geqslant 1$, 2) $g_n\in G_n$, 3) 如果$k>1$，元素g_k不是群G_{k-1}中任何元素在同构映射φ_{k-1}下的像，, 4) g_{n+1}是元素g_n在同构映射φ_n下的像，

$$g_n\varphi_n=g_{n+1}, n=k, k+1, \cdots.$$

如果已经给出了两个元素络

$$\gamma'=g'_k, g'_{k+1}, \cdots, g'_n, \cdots,$$

$$\gamma''=g''_l, g''_{l+1}, \cdots, g''_n, \cdots.$$

且$k\neq l$，则元素列

$$g'_m g''_m,\ g'_{m+1}g''_{m+1},\ \cdots,\ g'_n g''_n,\ \cdots, \tag{4}$$

其中 $m=\max(k, l)$，同样也是一个元素络. 事实上，

$$(g'_n g''_n)\varphi_n=(g'_n\varphi_n)(g''_n\varphi_n)=g'_{n+1}g''_{n+1},$$

而元素 $g'_m g''_m$ 不是 G_{m-1} 中任何元素在同构映射 φ_{m-1} 下的像，因为在两个因子中有一个是 G_{m-1} 中某一元素在 φ_{m-1} 下的像，而另一个不是. 我们称元素络(4)为这两个已知元素络的乘积，并用 $\gamma'\gamma''$ 表示它. 如果 $k=l$，则在同构映射 φ_{m-1} 下元素 $g'_m g''_m$ 可能在 G_{m-1} 中有原像. 在这一情况下，可以在序列(4)的前面添加若干个元素而将它补成一个元素络，并且这种添补法完全是唯一的. 由这样的方法得出的元素络将被看作乘积 $\gamma'\gamma''$.

这里定义的元素络乘法，其结合律可由群 G_n 中运算的结合律推出. 单位元是所有由群 G_n 中的单位元所组成的元素络. 元素络(3)的逆元素络是

$$g_k^{-1},\ g_{k+1}^{-1},\ \cdots,\ g_n^{-1},\ \cdots$$

因此，所有元素络的集合对于上面所定义的乘法构成一个群. 这个群我们记作 $\bar{G}$，它可以称作群列(1)对于同构映射(2)的*极限群*. 同样也可以说：群列(1)由同构映射(2)成为一个*递增序列*，而 $\bar{G}$ 则是这一递增序列的*并集*. 事实上，我们可以把所有那些包含群 G_s 中的一个元素的元素络，即从群 G_k，$k\leqslant s$，中的元素开始的元素络收集在一起. 这些元素络组成群 $\bar{G}$ 中一个与群 G_s 同构的子群 $\bar{G}_s$. 子群

$$\bar{G}_1,\ \bar{G}_2,\ \cdots,\ \bar{G}_n,\ \cdots \tag{5}$$

中，一个群嵌入另一个群的方式，正如利用同构映射(2)把(1)中的一个群嵌入另一个群的方式一样，递增子群列(5)的并集是整个群 $\bar{G}$.

给定了群(1)和同构映射(2)，群 $\bar{G}$ 就唯一地确定了. 如果只给出群(1)，这一点是作不到的. 事实上，有理数加法群 R 是一个

由无限循环群组成的可数递增序列的并集.——参看上文，例1.然而这一事实对二进分数加法群 R_2 也同样正确，因为这个群是它的子群

$$\{1\}\subset\left\{\frac{1}{2}\right\}\subset\left\{\frac{1}{4}\right\}\subset\cdots\subset\left\{\frac{1}{2^n}\right\}\subset\cdots$$

组成的递增序列的并集. 群 R 和 R_2 并不同构，因为，举例来说，在群 R_2 中没有一个元素 x 能适合方程

$$3x=1,$$

而在群 R 中这样的方程是可解的. 这一事实表明，递增群列的并集不但取决于这些群本身，而且和这些群中每一个群嵌入次一群中的方式有关.

刚才说明的这项构成法不难推广到任何一个具有任意势的、按任意方式排列的一组群. 只要假定，对于这一组群中任意两个群 G_α 和 G_β，其中第一个群位于第二个群之先，都定义了一个把群 G_α 映入群 G_β 的同构映射 $\varphi_{\alpha\beta}$，并且，如果同构映射 $\varphi_{\alpha\beta}$ 和 $\varphi_{\beta\gamma}$，因而同构映射 $\varphi_{\alpha\gamma}$ 均已定义，则施行 $\varphi_{\alpha\gamma}$ 的效果与接连施行映射 $\varphi_{\alpha\beta}$ 和 $\varphi_{\beta\gamma}$ 的效果相同. 这个构成法的细节留给读者自己去做. [见补充2.2]

现在我们要利用这一项构成法来构成一个在下文中，尤其是在阿贝尔群的理论中有极为重要作用的群. 假设已经给定一个素数 p，任何一个 p^n 阶循环群都包含一个唯一的 p^{n-1} 阶子群. 由此对于每一个整数 n，可以定义 p^{n-1} 阶循环群到 p^n 阶循环群内的同构映射. 因此我们可以讨论 p^n 阶 $(n=1,2,\ \cdots,)$ 循环群的递增序列. 这个序列的并集称为 p^∞ 型群[1]. 不难看出，p^∞ 型群和所有 $p^n(n=1,2,\cdots)$ 次单位根的乘法群同构.

因为对任何小于 n 的数 k，p^n 阶循环群 $\{a\}$ 有一个唯一的 p^k

1) 这个群有时称为半循环群.

阶循环子群 $\{a^{p^{n-k}}\}$,所以对于任何 $k, k=1, 2, \cdots$, p^∞ 型群 P 也有一个唯一的 p^k 阶循环子群，并且 P 和这些子群的递增序列的并集重合．假设这些子群是 $\{a_k\}, k=1, 2, \cdots$, 此外并命 $a_0=1$. 现在假定 U 是群 P 中任意一个真子群,那末它不能包含所有元素 a_i. 命 a_{n+1} 为第一个不包含在 U 内的生成元素．这时子群 U 就和子群 $\{a_n\}$ 重合．事实上,如果 U 中包含一个元素 a_k, $k>n+1$, 则整个循环子群 $\{a_k\}$ 都包含在 U 内，因而元素 a_{n+1} 包含在 U 内．如果 U 中有一个元素 b 不在 $\{a_n\}$ 内,那末就可以找出这样一个整数 $k, k>n$, 使得

$$b\in\{a_{k-1}\},\quad b\in\{a_k\}.$$

在这时等式

$$\{b\}=\{a_k\}$$

成立,就是说,元素 a_k 在 U 内.

这样就证明了，p^∞ 型群的任何一个真子群都是一个 p^n 阶有限循环群.

由第七章的结果可以得出，p^∞ 型群(对所有素数 p)是唯一的这样一种无限阿贝尔群，在其中所有真子群都是有限的．О. Ю. Шмидт提出过这样一个问题：是否存在具有这样性质的无限非交换群？这一问题迄今尚未解决[参看补充 16.5].

第三章 正规子群

§8. 一个群按其子群的分解

设已知群G的两个子集M和N. 所谓这这两个集的乘积MN，是指群G中所有能表成M中某一元素和N中某一元素的乘积的那样一些元素的集合[1]. 如果M和N这两个集合之一是由一个元素a所组成的，那末我们就得出一个元素和一个集合的乘积aN，或一个集合和一个元素的乘积Ma的定义.

子集的乘法满足结合律，

$$(MN)P=M(NP),$$

但一般说来不满足交换律. 如果对于某两个集合M和N等式

$$MN=NM$$

成立(这就是说，对任意两个元素a和b，$a\in M, b\in N$，可以找到这样两对元素$a', a''\in M$和$b', b''\in N$，使$ab=b'a', ba=a''b''$)，那末集合M和N就称为可换的. 这一情形的特例是一个元素和一个子群可换，两个子群可换等等.

可注意的是：在A和B都是群G的子群时，集合AB不一定是一个子群，也就是说，两个子群A和B的乘积AB一般说来并不等于§6中所定义的子群$\{A, B\}$. 我们只能断定

$$AB\subseteq\{A, B\}.$$

群G的子群A和B所生成的子群$\{A, B\}$与这两个子群的乘积AB相重合的充分必要条件是A与B可换.

事实上，如果

1) 一个元素可以同时等于好几个这种形式的不同乘积，但我们却不能因此而认为这个元素在集合MN中出现多次.

$$AB=\{A,B\},$$

则对于任意两个元素 $a\in A$ 和 $b\in B$，包含在$\{A,B\}$中的元素 ba应该等于某一元素 $a'b'$，$a'\in A$，$b'\in B$，这就是说

$$BA\subseteq AB;$$

在另一方面，我们可以证明元素 ab 包含在乘积 BA 内．事实上，我们可以利用上面已经证明了的包含关系而得出

$$(ab)^{-1}=b^{-1}a^{-1}=a''b'',\ a''\in A,\ b''\in B.$$

由此即有 $ab=b''^{-1}a''^{-1}$，也就是说 $BA\supseteq AB$，因而 $AB=BA$.

反过来，如果 A 和 B 可换，则任意一个 a_1ba_2 或 b_1ab_2 这种形式的三个元素的乘积都显然能够表成 $a'b'$ 这种形式，——在第一种情形只要利用 A 和 B 可换这个事实将 ba_2 换成一个和它相等的乘积 $a_2'b'$，然后命 $a_1a_2'=a'$ 即可；在第二种情形将 b_1a 换成 $a'b_1'$，然后命 $b_1'b_2=b'$．如果已经证明了任何从 A 和 B 中轮流取出的 n（$n\geqslant 3$）个因子的乘积都包含在 AB 内，并且给出了一个由 $n+1$ 个因子构成的同样的乘积，那末我们就可以将前面 n 个因子的乘积换一个和它相等的乘积 $a'b'$ 而重新回复到三个因子相乘的情形来．这就证明了子群$\{A,B\}$中任何一个元素都包含在集合 AB 内.

一个阿贝尔群中的所有子群当然都是彼此可换的．在一个（有限或无限）对称群中，具有下述性质的两个子群 A 和 B 同样也是可换的，即：任何一个符号，如果它在子群 A，B 之一的至少一个置换下被改变的话，那末它在另一个子群的所有置换下都不变．事实上，这两个子群中的元素本身将是可换的．其次，我们建议读者自己去证明，在三次对称群中，由置换

(123)和(12)

所生成的两个循环子群是可换的；而在同一群中由置换

(12)和(23)

所生成的两个循环子群则不可换.

为了今后的需要起见，我们在这里指出，如果A是群G的子群，则等式

$$AA=A$$

成立. 事实上，$AA\subseteq A$显然成立；但在另一方面A和1的乘积就已经给出全部的A.

群的子集的乘法在群按其子群的分解中有重要的应用，这种分解在整个群论中起着很重要的作用.

设已知群G的一个子群H. 如果a是G中一个任意的元素，则aH称为由元素a所决定的、群G对子群H的左陪集. 因为子群H包含单位元素，故元素a包含在左陪集aH内.

如果b是左陪集aH中一个任意的元素，则左陪集aH和bH相重合，也就是说，每一个左陪集都能由它里面的任意一个元素所决定. 事实上，如果$b=ah_0$, $b_0\in H$，则

$$bh'=a(h_0h'),\ ah''=b(h_0^{-1}h''),\ h',h''\in H.$$

因此，一个左陪集中任意一个元素都可以作这个陪集的代表元.

从这里就可以知道，群G对子群H的任意两个左陪集或者彼此重合，或者没有公共元素，即他们的交是一个空集. 这样，整个群G就分解成为一些对子群H的互不相交的左陪集. 这个分解称为群G对子群H的左侧分解. 这一分解中的左陪集之一就是子群H本身：如果a包含在H内，则$aH=H$.

注意，两个元素a和b属于群G对子群H的同一左陪集，当且仅当乘积$a^{-1}b$包含在子群H内.

下面这几个例子可以用来说明左侧分解的概念：

例1. 设G是整数加法群，H是由能被4整除的所有整数组成的子群. 两个整数a和b属于群G对子群H的同一左陪集的充分必要条件是：a和b被4除时所得的余数相同. 因此，G对H的左侧分解由四个左陪集构成：即子群H本身和被4除时余数分别是

1, 2, 3的整数所组成的三个集合.

例 2. 设G是三次对称群而$H=\{(12)\}$. G对H的左侧分解由三个陪集构成: 即由元素 1, (12)所组成的子群H本身; 由元素(13)和(132)所组成的陪集$(13)\cdot H$; 由元素(23)和(123)所组成的陪集$(23)\cdot H$.

例 3. 设G是实元素的n阶满秩矩阵所成的群, 而H是由行列式等于 1 的矩阵所组成的子群. 我们可以把行列式相等的矩阵归入同一陪集而得出G对H的左侧分解.

如果在任意群G中取群G本身作为子群H, 则G对H的左侧分解仅由一个陪集构成; 如果H是单位子群E, 则群G中的每一个元素都组成一个独立的陪集.

除左侧分解之外, 我们也可以把集合$Ha(a\in G)$称为群G对子群H的一个右陪集, 从而得出G对H的右侧分解. 上面关于左侧分解所讲到的各点, 都可以转到右侧分解上去. 特别, 子群H也是G对H的右陪集之一. 两个元素a和b属于群G对子群H的同一右陪集, 当且仅当$ba^{-1}\in H$.

对于阿贝尔群当然没有必要区别左侧分解和右侧分解. 在非交换群的情形这两种分解可能不相同. 例如三次对称群对子群$H=\{(12)\}$的右侧分解就和上面例 2 中所说到的左侧分解不相同. 这个分解由下面三个陪集所构成: 即子群H本身; 陪集$H\cdot(13)$, 出现于这个陪集中的元素有(13)和(123); 以及由元素(23), (132)所组成的陪集$H\cdot(23)$. 然而有一个事实却是可以肯定的, 即任何一个群G对于任意子群H的两种分解都由同样个数的陪集构成(在陪集个数为无限时这句话的意思是说, G对H左陪集和右陪集分别所成的集合有相同的势). 事实上, 左陪集aH中元素的逆元所组成的集合和右陪集Ha^{-1}相重合,

$$(aH)^{-1}=Ha^{-1};$$

这个关系式在左陪集和右陪集之间建立了一个相互单值对应.[参看补充2.3.]

在每一种分解中,群G对子群H的陪集的个数(在陪集的个数为无限的情形下则是这些陪集所成集合的势)称为子群H在群G中的**指数**. 如果陪集的个数是有限的, 那末H就称为一个**具有限指数的子群**.

在有限群中,并且只有在有限群中, 所有子群都有有限指数. 事实上, 单位子群的指数和整个群的势相等. 在无限循环群中所有不等于单位子群的子群都是具有限指数的子群, 并且对于任何一个自然数n,这个群包含一个,而且仅有一个,指数为n的子群. 这一命题的证明是以§6中所证关于循环群的子群的定理为依据的.

在另一方面,也存在这样的群,他们里面所有真子群的指数都是无限的. 例如有理数加法群R就是这样的一个群. 事实上, 如果H是群R中一个真子群,则在H之外可以找到一个元素a,使元素pa包含在H内,这里p是某一素数. 有理数

$$a, \frac{1}{p}a, \frac{1}{p^2}a, \cdots, \frac{1}{p^n}a, \cdots$$

都不包含在H内,且属于群R对子集H的不同的陪集. 事实上,如果

$$\frac{1}{p^n}a = \frac{1}{p^k}a + h, h \subset H, n > k,$$

则

$$a = p^{n-k}a + p^n h,$$

也就是说,a本身就包含在H内,而这是和我们的假定相违的.

Poincaré定理 *有限多个具有限指数的子群的交也具有限指数.*

显然只要对两个子群相交的情形证明这个定理就行了. 设子

群H和F在群G中有有限指数，而D是这两个子群的交. 两个元素a和b属于群G对子群D的同一左陪集，当且仅当$a^{-1}b\in D$，也就是说，当且仅当$a^{-1}b\in H$，$a^{-1}b\in F$. 因此，如果我们取群G对H的左陪集和对F的左陪集的所有非空交，我们就得出G对D的所有左陪集. 由于子群H和F的指数都是有限的，故这些交的个数也是有限的，因而D在G中的指数也是有限的. 我们还可以进一步断言，*D在群G中的指数不大于H和F在这个群中的指数的乘积*.

在有限群的情形，由一个群按其子群的分解这个概念还可以引出下面这个重要的定理：

Lagrange 定理 *在一个有限群中子群的阶和指数是这个群的阶的约数.*

事实上，如果有限群G的阶是n，而它的子群H的阶是k，指数是j，则群G对子群H的每一左陪集都由k个元素组成. 由此即得出

$$n=kj.$$

因为群中一个元素的阶等于这个元素所生成的循环子群的阶，故由拉格朗日定理可知，*有限群中任何一个元素的阶都是这个群的阶的约数*.

由 Lagrange 定理同时还可以看出，*任何一个素数阶的群都是循环群*. 事实上，这个群和它里面任意一个不等于1的元素所生成的循环子群相重合.

Lagrange 定理是下面关于任意群的一个定理的特例：

如果H和F是群G中两个具有有限指数的子群，且H包含在F内，又设n和j分别是H和F在群G中的指数，则子群H在子群F中的指数k同样也是有限的，并且

$$n=kj.$$

事实上，如果两个元素 a 和 b 包含在群 G 对子群 H 的同一左陪集内，那末他们也一定包含在 G 对子群 F 的同一左陪集内. 因此，群 G 对 F 的每一个左陪集都能分解成为群 G 对 H 的若干个完整的左陪集. 由这一点就已经看出 H 在 F 中的指数是有限的了. 如果 F 由群 G 对 H 的 k 个左陪集构成，则任何一个左陪集 $aF(a\in G)$ 同样也由 k 个这样的陪集构成：只要将所有出现在 F 的群 G 对 H 的左陪集从左边乘上 a，我们就可以得出这些陪集来. 这样一来，定理就完全被证明了.

如果 G 是有限群而 $H=E$，我们就得出 Lagrange 定理.

在群论中的某些问题上我们要利用群的双模分解. 双模分解是群对子群的陪集分解的推广. 设已知群 G 中两个任意的子群 H 和 K. 如果 a 是 G 中任意一个元素，则乘积 HaK 显然包含元素 a；这个乘积叫作由元素 a 所生成的、群 G 对双模 (H, K) 的陪集. 如果元素 b 包含在陪集 HaK 内，即 $b=hak$，则 $a=h^{-1}bk^{-1}$；换句话说，$a\in HbK$. 最后，由 $b\in HaK, c\in HbK$ 可得出 $c\in HaK$. 这就证明了群 G 可分解成为一些对双模 (H, K) 的互不相交的陪集. 这里所得出的群 G 的分解，在 $K=E$ 时即变成群 G 对子群 H 的右侧分解，而在 $H=E$ 时则变成群 G 对子群 K 的左侧分解.

显然，陪集 HaK 在包含其中的每一个元素的同时，也包含由这个元素所生成的群 G 对子群 H 的整个右陪集. 在出现于陪集 HaK 内的、G 对 H 的右陪集和群 K 对交 $D=a^{-1}Ha\cap K$ 的右陪集之间，可用下面的方法建立起一个相互单值对应：即令陪集 Dk_0 $(k_0\in K)$ 与陪集 Hak_0 相对应. 事实上，如果 $Hak_0=Hak_1$，$k_1\in K$，则 $k_1=a^{-1}ha\cdot k_0$，$h\in H$，由此即有 $a^{-1}ha\in D$，因而 $k_1\in Dk_0$. 另一方面，如果 $k'\in K$，则陪集 Dk' 将对应于出现在 HaK 中的陪集 Hak'. 如果进一步有 $Dk'=Dk''$，则存在元素 $h\in H$，使

$$k''=a^{-1}ha\cdot k',$$

换句话说，$ak''=hak'$，从这里即得出 $Hak''=Hak'$. 这样，由子群 $a^{-1}Ha\cap K$ 在 K 中的指数是有限的，可以得出陪集 HaK 中所包含的群 G 对 H 的右陪集的个数也是有限的，反过来也对，并且这两个数目相等.

§9. 正规子群

从上一节中我们知道，非交换群可能具有这样的一些子群，对它们的左侧分解和右侧分解并不相同. 但是任何一个群对单位子群(以及对这个群本身)的两种分解一定是一致的. 不难验证，上一节中的例 3 也给出了两种分解相一致的一个情形，而这种情形却不像上述那样明显了.

如果群 G 对子群 H 的左侧分解和右侧分解一致，则子群 H 称为群 G 的*正规子群*或*不变子群*.

换句话说，如果对于任何一个元素 a，由 a 所决定的群 G 对子群 H 的两个陪集——左陪集和右陪集——相一致：

$$aH=Ha,$$

则 H 是 G 的正规子群.

这个等式表明，*群 G 的子群 H 是 G 的正规子群的充分必要条件是：子群 H 和群 G 中任意元素可换，即对 G 中任意一个元素 a 和 H 中任意一个元素 h，在 H 中可找到这样的元素 h' 和 h''，使*

$$ah=h'a, ha=ah''. \tag{1}$$

正规子群的概念还可以用多种别的方法来定义；每一次我们都选取对所论情况用起来最方便的那一种定义. 现在我们举出两个这样的定义；以后还要给出另外几种定义.

设 a 和 b 是群 G 中的两个元素. 如果在 G 中至少可以找到这样的一个元素 g，使

$$b=g^{-1}ag,$$

则 a 和 b 称为在群 G 中共轭. 有时也说，b 可由 a 经元素 g 变形得出.

因为(1)中的第二个等式可以改写成

$$a^{-1}ha=h''$$

的形式，并且 a 和 h 分别是 G 和 H 中的任意元素，所以我们就得出了正规子群的下面一个性质：

群 G 的正规子群 H 在包含其中的每一个元素 h 的同时，也包含群 G 中一切与 h 共轭的元素.

这个性质可以用来作为正规子群的定义，并且常常在下面这个更一般的形式下用起来更为方便：

设在一个具生成系 M 的群 G 中，给出一个由元素集合 N 所生成的子群 H，如果 N 中任意元素经 M 中的元素及其逆元变形后都不超出 H 的范围，则 H 是 G 的正规子群.

事实上，不难验证等式：

$$g^{-1}(h_1^{\alpha_1}h_2^{\alpha_2}\cdots h_n^{\alpha_n})g=(g^{-1}h_1g)^{\alpha_1}(g^{-1}h_2g)^{\alpha_2}\cdots(g^{-1}h_ng)^{\alpha_n},$$

$$(g_1g_2)^{-1}h(g_1g_2)=g_2^{-1}(g_1^{-1}hg_1)g_2.$$

但是 G 中任何一个元素都有

$$g=g_1g_2\cdots g_k$$

的形式，其中 $g_i\in M$ 或 $g_i^{-1}\in M(i=1,2\cdots,k)$；而 H 中任何一个元素都有

$$h=h_1^{\alpha_1}h_2^{\alpha_2}\cdots h_n^{\alpha_n}$$

的形式，其中 $h_i\in N(i=1,2,\cdots,n)$. 因此我们永远有 $g^{-1}hg\in H$. 而这正是我们所要证明的.

不难看出，在 M 的所有元素都具有限阶的情形下，定理的陈述中提及 M 中元素的逆元是多余的.

如果 U 是群 G 的一个子群，而 g 是 G 中一个任意的元素，那末集合 $g^{-1}Ug$ 显然是由子群 U 中的元素经 g 变形后所得出的元素所

组成的，这个集合也是一个子群. 事实上，如果元素 u_1 和 u_2 属于 U，则

$$(g^{-1}u_1g)\cdot(g^{-1}u_2g)=g^{-1}(u_1u_2)g, \tag{2}$$
$$(g^{-1}u_1g)^{-1}=g^{-1}u_1^{-1}g.$$

子群 $g^{-1}Ug$ 称为群 G 中与 U 共轭的子群. 同样也说，子群 $g^{-1}Ug$ 是由子群 U 经元素 g 变形得出的. 因为由

$$g^{-1}u_1g=g^{-1}u_2g$$

可得出 $u_1=u_2$，故根据(2)我们可以断定映射

$$u\to g^{-1}ug, u\in U$$

是子群 U 到子群 $g^{-1}Ug$ 上的一个同构映射.

由上面关于与正规子群中的元素共轭的元素所讲的事实可知，群 G 中所有与正规子群 H 共轭的子群都应该全部包含在 H 内. 事实上，我们还可以更进一步地断言. 假如子群 $g^{-1}Hg$ 是正规子群 H 的真子群，也就是说，假如 H 中有一个不属于 $g^{-1}Hg$ 的元素 h_0，则与元素 h_0 共轭的元素 gh_0g^{-1} 将不会包含在 H 内. 在另一方面，因为群 G 中任何一个与其所有共轭子群相重合的子群，在包含其中每一个元素的同时也包含所有与这个元素共轭的元素，所以我们可以得出下面的结果:

群 G 的正规子群，并且仅有这样一种子群，重合于群 G 中所有与它共轭的子群.

现在让我们证明正规子群的定义的一些最简单的推论.

指数为 2 的子群是正规子群，因为对这个子群的两种分解是一致的. 例如 n 次交错群在同次对称群中的指数等于 2，所以它是这个群中的正规子群.

群 G 中任意一组正规子群的交也是这个群中的正规子群.

事实上，如果子群 D 是这些已知的正规子群的交，则与 D 中某一元素共轭的每一个元素也应同时包含在所有这些正规子群内，

因而也包含在它们的交内.

利用正规子群这一性质，我们可以像在§6中对子群的情形所作的那样，来讨论由群G中一个子集M所生成的正规子群. 这个正规子群是群G中所有包含子集M的正规子群的交.

群G中任意一组正规子群所生成的正规子群和这一组正规子群所生成的子群重合.

事实上，如果已知一组正规子群H_α(α遍历某一组足标)，则子群$\{H_\alpha\}$中的任何一个元素都可以写成

$$h_1h_2\cdots h_k$$

的形式，其中每一个因子h_i都包含在某一H_{α_i}内($i=1,2,\cdots,k$). 如果$g\in G$，则

$$g^{-1}(h_1h_2\cdots h_k)g=(g^{-1}h_1g)(g^{-1}h_2g)\cdots(g^{-1}h_kg);$$

但因为

$$g^{-1}h_ig\in H_{\alpha_i},\ i=1,2\cdots,k,$$

故与子群$\{H_\alpha\}$中某一元素共轭的每一个元素，本身也包含在这个子群内.

从这里可以知道，*群G中正规子群的一个递增序列的并集也是这个群的一个正规子群.* 这一点是很容易直接证明的.

正规子群既然与群中任意元素可换，当然也与这个群的任意子群可换. 由此根据§8可知，*由群G的正规子群H和任意子群F所生成的子群$\{H,F\}$与乘积HF相重合.* 换句话说，子群$\{H,F\}$中的任何一个元素可以表成乘积hf的形式，其中$h\in H$，$f\in F$，在同一前提下子群$\{H,F\}$也与FH重合.

如果H是群G的正规子群，而G的子群F包含整个H，

$$H\subset F\subset G,$$

则H*也是群F的正规子群.* 事实上，任何元素$f^{-1}hf$，$h\in H$，$f\in F$，属于H. 然而须注意的是：如果H是群G的正规子群，K是H

的正规子群，则K虽然是群G的子群，却不一定是G的正规子群．换句话说，一个群是另一个群的正规子群这一性质是不可传递的．下面我们可以见到许多这方面的例子．

阿贝尔群的任何一个子群都是正规子群．但是也存在所有子群都是正规子群的那种非交换群．所有这样的非交换群都称为Hamilton群，在Baer的论文[2]中可以找到关于这一类群的完全描述．特别，任何一个Hamilton群都含一个和下面这个群K同构的子群：群K称为四元数群，它本身也是一个Hamilton群．我们用K表示八次对称群中由置换

$$a=(1234)(5678)\text{和} b=(1537)(2846)$$

所生成的子群．

不难用直接置换的方法验证下面的关系式：

$$a^4=1, \tag{3}$$

$$b^4=1, \tag{4}$$

$$a^2=b^2, \tag{5}$$

$$aba=b. \tag{6}$$

从这些关系式我们可得出：

$$bab=a^3(aba)b=a^3b^2=a^5=a, \tag{7}$$

$$a^3b=b^2ab=ba, \tag{8}$$

$$b^3a=a^2ba=ab. \tag{9}$$

因为$a^2\cdot a=a\cdot a^2$，$b^2\cdot b=b\cdot b^2$，故利用关系式(5)我们可以用调换因子位置(即不减少因子的个数)的方法，将元素a和b的任何一个幂积表成这两个元素的一次幂交替出现的乘积，另外可能还要从左边乘上一个a^3或b^3；另一方面，只要这样一个乘积不和下面八个乘积之一相合，我们就可以利用(6)，(7)，(8)和(9)来减少它的因子个数．这八个乘积是：

$1, a, b, ab=(1836)(2745), ba=(1638)(2547),$

$a^2=b^2=(13)(24)(57)(68)$, $a^3=(1432)(5876)$,

$b^3=(1735)(2648)$;

但这八个乘积是八个不同的元素，故 K 是一个八次非交换群.

根据 Lagrange 定理，群 K 中任何一个不等于 E 或 K 本身的子群，其阶必为 2 或 4. 事实上 K 中有一个唯一的 2 阶子群即 $\{a^2\}$，和三个 4 阶子群，即 $\{a\}$, $\{b\}$ 和 $\{ab\}$. 如果我们用元素 a 和 b 去作这四个循环子群的生成元的变形，那末利用(3)—(7)我们就可以发现，所有这四个子群都是 K 的正规子群.

单纯群　对任何一个群来说，这个群本身和单位子群都是它的正规子群. 除了这两个正规子群之外不再有其他正规子群的群，称为*单纯群*. 单纯群是在某种意义上和 Hamilton 群相对立的一类群.

一个阿贝尔群是单纯群，当且仅当它是一个循环群，并且它里面的每一个不等于 1 的元素都是它的生成元. 因此，根据 § 6 中所作的关于循环群生成元的按语可以断定：*一个阿贝尔群是一个单纯群的充分必要条件是：这个群是一个循环群，并且它的阶数是一个素数.*

然而，不论是有限的或无限的非交换单纯群都是存在的. 举例来说，我们有下面这样一个定理，这个定理在 Galois 理论中起着很大的作用：

定理. *当 $n\geqslant5$ 时，n 次交错群 A_n 是单纯群.*

先证明下面两个引理：

引理 1. *如果 $n\geqslant3$，则由群 A_n 中长度为 3 的一切循环所生成的子群和整个群 A_n 重合.*

事实上，任何一个偶置换都是偶数个对换的乘积；但两个不相同的对换，其乘积或者等于一个长度为 3 的循环，或者等于两个这样的循环的乘积：如果 $\alpha, \beta, \gamma, \cdots\cdots$ 是被置换的符号，则

$$(\alpha\beta)(\alpha\gamma)=(\alpha\beta\gamma),$$

$$(\alpha\beta)(\gamma\delta)=(\alpha\beta\gamma)(\alpha\delta\gamma).$$

在另一方面，每一个长度为 3 的循环都是偶置换，因而包含在 A_n 内.

引理 2. 如果 $n\geqslant5$，则群 A_n 中任何至少包含一个长度为 3 的循环的正规子群都与整个群 A_n 相重合.

设群 A_n 的正规子群 H 包含一个长度为 3 的循环 $(\alpha\beta\gamma)$，而 $(\bar\alpha\bar\beta\bar\gamma)$ 是 A_n 中任意另一长度为 3 的循环. 如果符号 δ 和 ε 不同于符号 α,β 和 γ，则 n 次置换

$$a=\begin{pmatrix}\cdots\alpha\cdots\beta\cdots\gamma\cdots\delta\cdots\varepsilon\cdots\\ \cdots\bar\alpha\cdots\bar\beta\cdots\bar\gamma\cdots\delta'\cdots\varepsilon'\cdots\end{pmatrix}$$

在必要时可以对调第二行中符号 δ' 和 ε' 的位置而成为一个偶置换，具有性质

$$a^{-1}(\alpha\beta\gamma)a=(\bar\alpha\bar\beta\bar\gamma).$$

因此正规子群 H 包含群 A_n 中所有长度为 3 的循环；根据引理 1，H 和整个群 A_n 相重合[1].

现在我们来证明定理本身. 设群 A_n 有一个异于 E 的正规子群 H，并设 H 中有这样的元素，当它们被分解为循环的乘积时，至少有一个循环的长度 $\geqslant4$. 设 h 是这样的元素中的一个：

$$h=(\alpha\beta\gamma\delta\cdots)\cdots,$$

这里括号外面的点表示其余的循环. 这时，在群 A_n 中与 h 共轭的元素

$$h'=(\alpha\gamma\beta)h(\alpha\beta\gamma)=(\beta\gamma\alpha\delta\cdots)\cdots$$

也属于 H，因而元素

$$h^{-1}h'=(\alpha\beta\delta)$$

1) 用直接的验算可以证明，在 $n<5$ 时引理 2 也是正确的.

属于 H. 因此，根据引理 2, $H=A_n$.

现在设H中某一元素 h 的循环分解式中只有长度为 3 的，或者可能只有长度为 2 的循环出现. 我们将假定这个分解式中长度为 3 的循环不少于两个；因为不然的话，h^2 就是一个长度为 3 的循环，那就可以直接应用引理 2 了. 如果

$$h=(\alpha\beta\gamma)(\alpha'\beta'\gamma')\cdots,$$

则元素

$$h'=(\beta'\alpha'\gamma)h(\gamma\alpha'\beta')=(\alpha\beta\alpha')(\gamma\gamma'\beta')\cdots$$

也包含在H内，因而元素

$$hh'=(\alpha\alpha'\gamma\beta\gamma')\cdots$$

包含在H内；这个元素含有一个长度为 5 的循环，这样我们又回到了前面的情形.

最后，设正规子群H里某一元素 h 的循环分解式中只包含长度为 2 的循环；这样的循环的个数当然是一个偶数. 如果 $h=$ $=(\alpha_1\beta_1)(\alpha_2\beta_2)$，则元素

$$h'=(\gamma\beta_1\alpha_1)h(\alpha_1\beta_1\gamma)=(\beta_1\gamma)(\alpha_2\beta_2)$$

也包含在H内，这里的 γ 是任意一个既不同于 α_1, β_1 也不同于 α_2, β_2 的符号. 在这时，元素

$$hh'=(\alpha_1\gamma\beta_1)$$

包含在正规子群H内，因而 $H=A_n$. 如果

$$h=(\alpha_1\beta_1)(\alpha_2\beta_2)(\alpha_3\beta_3)(\alpha_4\beta_4)\cdots,$$

则元素

$$h'=(\beta_1\alpha_2)(\beta_2\alpha_3)h(\beta_2\alpha_3)(\beta_1\alpha_2)=(\alpha_1\alpha_2)(\beta_1\alpha_3)(\beta_2\beta_3)(\alpha_4\beta_4)\cdots$$

包含在H内，因而元素

$$hh'=(\alpha_1\alpha_3\beta_2)(\alpha_2\beta_3\beta_1)$$

也包含在H内；这就使得我们重新回到前面讨论过的情形. 这样

一来，定理就完全被证明了[1]。

$n\geqslant 5$ 这一假定是不可缺少的. 虽然三次交错群是一个三次循环群，因而是一个单纯群；可是四次交错群不是单纯群——不难验证，置换(12)(34)，(13)(24)，(14)(23)和元素1一道组成 A_4 中一个正规子群. 这个正规子群是一个4阶阿贝尔群，但不是循环群.

上面所证明的定理表明，有无限多个非交换的有限单纯群存在. 但非交换有限单纯群远不只限于交错群. 全面决定所有有限单纯群这样一个问题还未完全解决，在§61中要给出一些关于这一问题的有关结果.[2]

在上面的证明中没有一处用过群 A_n 是有限群这一事实，因此我们可以断定，可数交错群或，更一般地，具任意无限势(参看§4，例14)的交错群是单纯群. 这就是说，存在具任意无限势的单纯群. [参看补充2.4.]

§10. 正规子群与同态及商群的关系

由正规子群的定义可知，群 G 对正规子群 H 的左陪集同时也是右陪集，反之亦然. 这样我们就只说群 G 关于正规子群 H 的陪集和 G 按这个正规子群的分解.

群 G 按正规子群 H 的分解是这个群的一个正则分解.

事实上，设已知群 G 对正规子群 H 的两个陪集. 如果从这两个陪集中任意取出两个代表元 a 和 b，也就是说，如果这两个陪集能表作 aH 和 bH，则根据群中子集乘法的结合律和等式 $Hb=bH$，$HH=H$，我们可得出

1) 这个定理还有几个证明和书中所叙述的证明在性质上极为相近，就是先从 H 中选出一个不等于单位元的元素，它使尽可能多的符号不变. 这一类证明中的最简单的一个可以在鲍埃尔 Bauer 的工作[1]中找到。

2) 截至准备第三版时，这个问题已经取得重大的进展.（有限单群的分类问题已经解决. 可参看，例如D. Gorenstein, *Finite Simple Groups*, *Plenum Press NY*, 1982——译者）

$$aH\cdot bH=abHH=abH.$$

这一命题的反面也是正确的：

如果已知群 G 的任意一个正则分解，则在这一分解下包含单位元素的那个类是群 G 的一个正规子群，而其余的类则是群 G 对这个正规子群的陪集.

设在这个分解下 A 是包含元素 1 的类. 如果 a_1 和 a_2 是 A 中的任意两个元素，则根据正则分解的定义，乘积 a_1a_2 应和乘积 $1\cdot1=1$ 属于同一类. 因此，

$$a_1a_2\in A.$$

其次，如果 a 是类 A 中任意一个元素，则乘积 $aa^{-1}=1$ 应和乘积 $1\cdot a^{-1}=a^{-1}$ 属于同一类. 由此即有

$$a^{-1}\in A.$$

这就证明了 A 是 G 的一个子群. 再次，如果 a 是 A 中任意一个元素,而 b 是 G 中任意一个元素，则乘积 $b^{-1}ab$ 应和乘积 $b^{-1}1\cdot b=1$ 属于同一类,这就是说，$b^{-1}ab\in A$. 因此，类 A 是群 G 的一个正规子群.

最后,设 B 是在这一正则分解下的任意一个类.如果 b 是 B 中的一个元素,则对 A 中任意元素 a，乘积 ba 和乘积 $b\cdot1=b$ 属于同一类. 因此整个陪集 bA 全包含在 B 内. 现在设 c 是 B 中另一任意元素. 因为 b 和 c 在这个正则分解下属于同一元素类，故 $b^{-1}c$ 和 $b^{-1}b=1$ 也属于同一元素类,也就是说

$$b^{-1}cA\in A.$$

由此即有

$$c\in bA.$$

这样我们就得出等式

$$B=bA,$$

定理完全证明.

上面这两个结果在群G的所有正则分解和这个群的所有正规子群之间建立了一个相互单值的对应关系，因而使得我们今后可以不必区别一个群的正则分解和这个群按其正规子群的分解. 特别,如果A是在群G的某一正则分解下包含单位元素的类,那末我们就可以不说群G对这一正则分解的商群，而说它对正规子群A的商群，并将这个商群记作$\frac{G}{A}$.

我们建议读者根据这个观念相应地改变群的同态定理(§3)的表述方式. 这个定理说明群的正规子群和它的同态映射之间建立了一个密切的关系. 正是由于这一关系，正规子群的概念才成为群论中最主要的概念之一. 特别，从这里我们还能得出正规子群的一个新的定义. 设φ是将群G映到群G'上的一个同态映射. 群G中被φ映到群G'的单位元素上去的全体元素叫做同态映射φ的核. 由同态定理和本节中的结果可引出下面的命题:

群G中的正规子群,并且只有这一类子群,才是这个群的同态映射的核.

若某一群G同态地映到群G'上,且若U是G的一个子群,则U也同样受到一个同态映射. 因此,在映射φ下子群U在群G'的象是G'的一个子群. 反之,如果U'是群G'的任意一个子群，则U'在群G中的完全原象U——即群G中所有被φ映入子群U'的元素的集合——是G的一个子群. 事实上，如果a和b是U的两个元素,即

$$a\varphi=a'\in U',\ b\varphi=b'\in U',$$

则
$$(ab)\varphi=a'b'.$$

但因$a'b'\in U'$,故元素ab应属于子集U. 其次,我们有

$$(a^{-1})\varphi=a'^{-1},$$

但$a'^{-1}\in U'$，故$a^{-1}\in U$. 这样就证明了我们的命题. 还可以补充

一点：因为子群 U' 包含群 G' 的单位元素，故 U' 的完全原像 U 包含同态映射 φ 的核．群 G 和 G' 的子群之间的这一对应关系还有其他许多重要的性质．这些性质都归并在下面的定理里，这个定理称为在同态映射下子群的对应定理．根据群的同态定理，在这个定理中我们将讨论群 G 的商群 $\bar{G}=\frac{G}{H}$ 和将群 G 映成这个商群的自然同态映射 φ．

如果使商群 $\bar{G}=\frac{G}{H}$ 中的每一个子群和这个子群在映射 φ 下在 G 中的完全原象相对应，则这一对应是群 $\bar{G}$ 中所有子群和群 G 中所有包含正规子群 H 的子群之间的一个相互单值对应．在这里，相互对应的子群在各自所属的群中的指数相同．最后，如果这两个子群中的一个是正规子群，则另一子群也是正规子群；且群 G 和 $\bar{G}$ 对这两个正规子群的商群同构．

证明：如果 $\bar{U}_1$ 和 $\bar{U}_2$ 是 $\bar{G}$ 中的两个互不相同的子群，那末在这两个子群中的一个里，譬如说，在子群 $\bar{U}_1$ 里，我们可以找到一个元素 $\bar{\alpha}$，使其不属于另一子群．在自然同态映射 φ 下，群 G 中有一些元素被映成元素 $\bar{\alpha}$，因此 $\bar{U}_1$ 和 $\bar{U}_2$ 这两个子群在 G 中的完全原象不可能重合．另一方面，设 U 是群 G 中任意一个包含 H 的子群，$\bar{U}$ 是 U 在 $\bar{G}$ 中的象，而 U_0 则是子群 $\bar{U}$ 在群 G 中的完全原象．包含式 $U\subseteq U_0$ 显然成立．如果 a_0 是 U_0 中的一个元素，则子群 U 中必有一个元素 a 和 a_0 属于群 G 对 H 的同一陪集，但因为 $H\subset U$，故 $a_0\in U$；因而 $U_0=U$．这就证明了我们所讨论的对应是一个相互单值对应．

现在设包含 H 的子群 U 和子群 $\bar{U}$ 是群 G 和 $\bar{G}=\frac{G}{H}$ 中相互对应的两个子群．对群 G 中的任意两个元素 a 和 b，元素 $a^{-1}b$ 属于子群 U，当且仅当陪集

$$a^{-1}bH = a^{-1}H \cdot bH$$

属于子群 $\overline{U}$. 这个事实表明，群G对子群U的左陪集和群$\overline{G}$对子群$\overline{U}$的左陪集之间有一个相互单值对应关系. 由此可知，子群U在群G中的指数和子群$\overline{U}$在群$\overline{G}$中的指数相等.

其次，设$\overline{U}$是$\overline{G}$的正规子群，φ和$\overline{\varphi}$分别是将G映成$\overline{G}$，将$\overline{G}$映成$\frac{\overline{G}}{\overline{U}}$的自然同态映射. 依次作映射$\varphi$与$\overline{\varphi}$可得出一个同态映射，将$G$映成$\frac{\overline{G}}{\overline{U}}$. 这个同态映射的核由群$G$中被$\varphi$映入子群$\overline{U}$的元素组成，这就是子群$U$的全部元素，因此，$U$是群$G$的正规子群，且

$$\frac{G}{U} \simeq \frac{\overline{G}}{\overline{U}}.$$

另一方面，如果U是群G的一个包含H的正规子群，而$\overline{U}$是群$\overline{G}$中和U相对应的子群，则对任何$\overline{u} \in \overline{U}$，$\overline{g} \in \overline{G}$，元素(即$G$对$H$的陪集)$\overline{g}^{-1}\overline{u}\overline{g}$由群$G$中属于$U$的元素组成，因而包含在$\overline{U}$内. 由此可知，$\overline{U}$是$\overline{G}$中的正规子群. 这样一来，定理就完全被证明了.

在 § 4 中曾举出群的同态映射的许多例子. 读者不难找出这些同态映射的核，并求出相应的商群. *现在让我们来定出有限和无限循环群的所有商群*.

设已知一个将循环群$A=\{a\}$映到某一群B上的同态映射φ. 如果

$$a\varphi = b,$$

则B中所有元素显然都是元素b的幂，也就是说$B=\{b\}$. 换句话说，*循环群的所有商群都是循环群*.

特别，设A是一个无限循环群，并将它看作整数加法群. 如果我们把元素b^k看作整数k的象，我们就得到一个将群A映到以元素b为生成元的n阶循环群B上的同态映射. 整数k和l被映成循环群B中同一个元素，当且仅当他们的差$k-l$能被n整除，或

如通常所说的，整数 k 和 l 对模 n 同余(记号：$k\equiv l(\mathrm{mod}\,n)$)．整数加法群的这一同态映射，相应于将整数加法群分解成按 n 的倍数所组成的子群的陪集；这些陪集即对模 n 的同余类[1]．利用§6中关于循环群的子群的结果，并命 n 遍历所有自然数，我们可得出结论：所有循环群，并且只有这些群，是无限循环群(即整数加法群)的商群，并且这个群对不同子群的商群互不同构[2]．

如果 $A=\{a\}$ 是一个 s 阶循环群，且 t 是 s 的一个约数：

$$s=tq,$$

则 A 的子群 $\{a^t\}$ 的阶数是 q，因而 A 对这个子群的商群是一个 q 阶循环群．在另一方面，因为一个有限群的商群的阶等于相应的正规子群的指数，因而永远是这个群的一个约数，所以我们可作出结论：s 阶有限循环群的商群是，而且仅是那样一些循环群，它们的阶是 s 的一个约数．

现在让我们求出 p^∞ 型群 P 的商群．

在§7中已经证明，组成下面这个递增序列的诸子群就是群 P 中的全部真子群：

$$E\subset\{a_1\}\subset\{a_2\}\subset\cdots\subset\{a_n\}\subset\cdots,$$

并且这些子群的阶分别是 $1,\ p,p^2,\cdots,p^n,\cdots$．现在让我们考察群 P 对子群 $\{a_n\}$ 的商群．这个商群是商群 $\frac{\{a_k\}}{\{a_n\}}$ 的递增序列的并集 $(k=n+1,n+2,\cdots)$．由上文中所述可知，商群 $\{a_k\}/\{a_n\}$ 是 p^{k-n} 阶循环群 $(k=n+1,n+2,\cdots)$．因此，商群 $\frac{P}{\{a_n\}}$ 也是一个 p^∞ 型群．这样我们就看到，p^∞ 型群和它的所有对于真子群的商群同构．

设已知两个群 A 和 B，如果在一个群 G 中可以找到一个和 A

1) 参看§8中当 $n=4$ 时的特例(例1)．

2) 在这里我们只说子群而不说正规子群，因为我们所讨论的群是一个阿贝尔群．

同构的正规子群 A'，使群 G 对 A' 的商群与 B 同构：

$$A' \simeq A,\quad \frac{G}{A'} \simeq B,$$

则群 G 称为群 A 借助于群 B 的扩张.

我们要指出：*在群 A 和 B 给定之后，群 G 并不是唯一地确定的*. 下面的例子可以说明这一事实.

例 1. 在 4 阶循环群 $\{a\}$ 中，子群 $\{a^2\}$ 是一个 2 阶循环子群；群 $\{a\}$ 对这个子群的商群同样也是一个 2 阶循环群. 然而如果我们取 4 阶非循环阿贝尔群 V 加以考察——正如 § 9 中所指出的,这个群包含在交错群 A_4 内——，那末我们就可以发现，这个群中任何一个循环子群的阶都是 2，并且群 V 对这个子群的商群也同样是一个 2 阶循环群. 这样一来，在我们面前就出现了一个 2 阶循环群借助于它本身的两种不同构的扩张.

例 2. 6阶循环群有一个唯一的 3 阶循环子群，它对这个子群的商群是一个 2 阶循环群；但三次对称群 S_3 的正规子群 A_3 也是一个 3 阶循环群，且商群 $\frac{S_3}{A_3}$ 也是一个 2 阶循环群.

在第十二章中将对群的扩张作详细的研究.

下面的定理在今后极为有用：

同构定理 *设 A 和 B 是群 G 的两个子群，且 A 是子群 $\{A, B\}$ 的正规子群，则这两个子群的交 $A \cap B$ 是 B 的正规子群，且*

$$\frac{\{A, B\}}{A} \simeq \frac{B}{(A \cap B)}.$$

事实上，因为 A 是 $\{A, B\}$ 的正规子群，故 $\{A, B\} = AB$. 因此，群 $\{A, B\}$ 对子群 A 的每一个陪集中都含有 B 中的元素，即和 B 有非空交. 由此可知：在将群 $\{A, B\}$ 映成商群 $\frac{\{A, B\}}{A}$ 的自然同态映射下，子群 B 将被同态地映成整个这个商群. 因此，根据同态定理，

商群$\frac{\{A,B\}}{A}$和群B对其正规子群(由B中所有被映成单位元素的元素所组成)的商群同构. 但B的这些元素就是交$A\cap B$中的全部元素. 定理得到证明.

还要强调一点: 在同构定理中包含着下面这样一个很容易直接证明的命题.

一个正规子群和一个子群的交是这个子群的正规子群.

现在让我们利用这个命题来证明下面的定理:

一个由单纯群所构成的递增序列的并集是一个单纯群.

事实上,设群G是它的真子群的递增序列

$$U_1\subset U_2\subset U_3\cdots\subset U_n\subset\cdots$$

的并集,并且这些子群都是单纯群;设H是群G的一个不等于E的正规真子群. 于是就存在这样一个下标k, 使交$U_k\cap H$既不等于E,也不等于U_k. 但根据上述,这个交是群U_k的一个正规子群,这和U_k的单纯性相矛盾.

同构定理是下面这个以 Zassenhaus 引理[1]为名的定理的一个特例.

设已知群G的子群A, A', B和B'; 且A'是A的正规子群, B'是B的正规子群, 则$A'(A\cap B')$是$A'(A\cap B)$的正规子群, $B'(B\cap A')$是$B'(B\cap A)$的正规子群,且相应的商群同构:

$$\frac{A'(A\cap B)}{A'(A\cap B')}\simeq\frac{B'(B\cap A)}{B'(B\cap A')}.$$

证明. 先引入下面的记号:

$$C=A\cap B$$

$$D=(A\cap B')(B\cap A').$$

显然$D\subseteq C$. 其次,因为B'是B的正规子群,而C是B的子群, 故

$$C\cap B'=A\cap B\cap B'=A\cap B'$$

是C的正规子群. 由于对A和B所作的假定是对称的,故交$B\cap A'$也是C的正规子群,因而D是C的正规子群,因为两正规子群的乘积还是一个正规子群. 这样一来,我们就可以讨论C对D的商群,并将它记作H,

$$H=\frac{C}{D}.$$

在另一方面,A'是A的正规子群, 因而乘积$A'(A\cap B)=A'C$是一个子群.这乘积中的任一个元素都具有形式$a'c$, 其中$a'\in A'$, $c\in C$. 我们使陪集(即群H中的元素)Dc和这个元素相对应. 如果元素$a'c$能用另一种方式表成下面的形式

$$a'c=a_1'c_1,$$

则

$$a_1'^{-1}a'=c_1c^{-1}\in(A'\cap C)\subseteq(A'\cap B)\subseteq D.$$

因而
$$c_1=(a_1'^{-1}a')c\in Dc.$$

这样我们就得出将群$A'C$映入群H的一个单值映射; 因为在这个映射下C中的每一个元素被映成它所属的陪集Dc,故群$A'C$被映成整个群H.这映射是一个同态映射:因为A'是$A'C$的正规子群,故

$$a_1'c_1\cdot a_2'c_2=a_3'(c_1c_2),\quad 其中\ a_3'\in A'.$$

子群$A'(A\cap B')$显然包含在这个同态映射的核内,因为我们知道$A\cap B'\subseteq D$. 另一方面, 如果元素$a'c$被这个映射映入D, 则$c\in D$,也就是说,

$$c=uv,\ 其中\ u\in(B\cap A'),v\in(A\cap B'),$$

但在这时

$$a'c=(a'u)v=a_1'v\in A'(A\cap B').$$

因此, 这个同态映射的核和子群$A'(A\cap B')$重合. 根据同态定理,由这个事实即可引出同构关系

$$\frac{A'(A\cap B)}{A'(A\cap B')}\simeq H.$$

由所考虑的子群的对称性可知,同构关系

$$\frac{B'(B\cap A)}{B'(B\cap A')}\simeq H$$

也成立．由此可得出引理中的全部断言．

在 $A\supseteq B, B'=E$ 时,即可由 Zassenhaus 引理得出同构定理．

在群 G 的子群 A 和 B 二者中没有一个被假定是 $\{A, B\}$ 的正规子群的情形,同构定理可化为关于 A 在 $\{A, B\}$ 中的指数和 $A\cap B$ 在 B 中的指数的某种说法．在一般的情形下只能断定这里的第一个指数不小于第二个指数．事实上，只要把证明同构定理时所使用的各个论点重复说一下,我们可以看出,子群 B 对子群 $A\cap B$ 的每一个右陪集都是 $\{A, B\}$ 对 A 的某一个右陪集和 B 的交．但 $\{A, B\}$ 对 A 的某些右陪集和 B 的交可能是空集——只要取 3 次对称群中的两个 2 阶循环群作为 A 和 B,就可以证实这一点．利用 § 8 中所证明的命题——$\{A, B\}=AB$,当且仅当 A 和 B 可换——,我们不难证明: $\{A, B\}$ 对 A 的每一个陪集都和 B 有非空交的充分必要条件是 A 和 B 可换．换句话说,如果假定所讨论的指数都是有限的,我们可得出下面的定理:

子群 A 在子群 $\{A, B\}$ 中的指数和子群 $A\cap B$ 在 B 中的指数相等的充分必要条件是 A 和 B 可换．

§ 11. 共轭元素类与共轭子群类

如果 M 是群 G 的一个子集，则群 G 中所有与 M 可换的元素组成群 G 的一个子群,这个子群称为集合 M 在群 G 中的*正规化子*．事实上,如果 $aM=Ma, bM=Mb$,则

$$(ab)M=aMb=M(ab);$$

其次，将等式 $aM=Ma$ 的两端从左右两边同时乘上 a^{-1}，我们可得出

$$Ma^{-1}=a^{-1}M.$$

特别，有了这个一般的定义，我们就可以讨论一个子群的正规化子或一个单独的元素的正规化子. 因为每一个元素必和它自己可换，每一个子群和它所包含的每一个元素可换，故元素 a(子群 A)的正规化子包含这个元素 a (子群 A)本身. 显然，子群 A 的正规化子是群 G 中包含 A 作为正规子群的最大子群. 由此可知，子群 A 的正规化子和整个群 G 相重合，当且仅当 A 是 G 的一个正规子群. 在另一方面，也可能有这样一种情形，即一个子群和它的正规化子相重合. 例如 3 次对称群中的 2 阶循环子群 $\{(12)\}$ 就有这样的性质.

元素 a 在群 G 中的正规化子显然包含在循环子群 $\{a\}$ 的正规化子内，但不一定和它相重合. 3 次对称群中元素 (123) 就能给出这样一个例子. 但在任何情况下，元素 a 的正规化子包含子群 $\{a\}$ 作为其正规子群.

正规化子的概念在建立本节所讲共轭元素和共轭子群的某些极重要的性质时，起着辅助的作用.

如果群 G 中的元素 b 和元素 a 共轭，即 $b=g^{-1}ag$，则 $a=gbg^{-1}$，也就是说，元素 a 可由元素 b 经元素 g^{-1} 变形得出. 因为 $a=1^{-1}a1$，故任何一个元素和它自己共轭. 最后，如果 $b=g_1^{-1}ag_1$，$c=g_2^{-1}bg_2$，则

$$c=(g_1g_2)^{-1}a(g_1g_2).$$

这就是说，元素共轭的性质是传递的. 由此可知，整个群 G 可分解成为若干个由一些彼此共轭的元素所组成的互不相交的集合，或如通常所说的，分解成为一些共轭元素类. 出现在同一共轭元素类中的元素显然有相同的阶.

§9中所给出的正规子群的定义之一现在可用下述方式表达出来：正规子群就是群G中的那样一种子群，他们在包含其每个元素的同时，也包含这个元素所属的整个共轭元素类；因此，正规子群也就是由群G中若干个完整的共轭元素类所构成的子群.注意：在一个群中，任何一个由这个群中的若干个完整的共轭元素类所构成的子集称为一个不变子集.

现在让我们给出共轭元素类的一些基本性质.

在群G中和元素a共轭的元素的个数，等于元素a在G中的正规化子N的指数.

事实上，如果$b=g^{-1}ag$，那么对N中的任何一个元素n，有$(ng)^{-1}a(ng)=b$.另一方面，如果$g_1^{-1}ag_1=b$,则$(gg_1^{-1})^{-1}a(gg_1^{-1})=a$,也就是说,$gg_1^{-1}\in N$,因而元素$g$和$g_1$包含在$G$对$N$的同一右陪集内. 因此，在$G$对$N$的右陪集和与$a$共轭的元素之间存在一个相互单值对应.

由此作为一个特例可知：群G的元素a包含在一个有限共轭元素类内，当且仅当这个元素的正规化子在群G中有有限指数.因为在一个有限群中，子群的指数是整个群的阶的约数(参看§8中的Lagrange定理)，故由上面所证明的定理可以推出，在一个有限群中，一个共轭元素类中元素的个数是这个群的阶的约数.

下面的命题是在§9开头时所证明的定理的一个特例：

由群G中某一共轭元素类，或者更一般地，由G中某一不变子集所生成的子群是G的正规子群.

由此不难证明，由群G中一个子集M所生成的群G的正规子群，就是由所有G内与M中元素共轭的元素所组成的集合$\overline{M}$所生成的子群.

群G中两个共轭元素类K_1和K_2的乘积由G中若干个完整的共轭元素类构成，也就是说，乘积K_1K_2是一个不变集合.

事实上，如果 $a_1 \in K_1$，$a_2 \in K_2$，则

$$g^{-1}(a_1a_2)g=(g^{-1}a_1g)(g^{-1}a_2g),$$

也就是说，和 K_1K_2 中元素共轭的元素也包含在这个乘积内.

最后还可以注意，如果 K 是群 G 的一个共轭元素类，则 K^{-1}，即 K 中元素的逆元素所组成的集合也是一个共轭元素类. 更一般地，对任意整数 s，K 中所有元素的 s 次幂所组成的集合也是群 G 的一个共轭元素类.

事实上，如果 $a_2=g^{-1}a_1g$，则 $a_2^s=g^{-1}a_1^sg$；而由 $b=g_1^{-1}a_1^sg_1$ 可得出 $b=(g_1^{-1}a_1g_1)^s$，即 b 是一个和 a_1 共轭的元素的 s 次幂.

在任何一个群 G 中，元素 1 组成一个单独的共轭元素类. 群 G 还可能有其他的能够单独组成共轭元素类的元素；这样的元素显然就是和群 G 中所有的元素都可换的那些元素，或者如通常所说的，是群 G 中的*不变元*. 不变元也可以定义为其正规化子和整个群相重合的元素.

不难看出，群 G 中所有不变元的集合 Z 是 G 的一个子群，这个子群称群 G 的*中心*，它是 G 的一个正规子群(因为它里面的每一个元素已经是一个完整的共轭元素类). 中心里的任何一个子群同样也是群 G 的正规子群. 阿贝尔群，并且只有阿贝尔群，和自己的中心相重合. 在另外一方面，也存在这样一种群，他们的中心仅由元素 1 组成. 这样的群有一个不完全准确，但非常便利的名称——*无中心群*. 例如对称群 $S_n(n\geqslant 3)$ 和所有非交换单纯群都是这样的群.

高等代数课程中有一个熟悉的定理表明：在系数属于某一域的满秩 n 阶矩阵的群中，中心由所有纯量矩阵组成，而所谓纯量矩阵，即是主对角线以外所有元素都等于零，而主对角线上元素彼此相等的那种矩阵.

可注意的是：群 G 对其中心的商群不一定是一个无中心群. 例如四元数群的中心是一个 2 阶循环群(参看 §9)，但四元数群对这

个子群的商群甚至还是一个阿贝尔群. 然而必须指出，一个非交换群对其中心的商群不可能是一个循环群. 事实上，如果商群$\frac{G}{Z}$是一个循环群，那末我们就可以从作为这个循环群的生成元的那个陪集中取出一个元素a_0来，这个元素和中心Z一道所生成的子群和整个群G相重合. 但因这里所涉及到的元素都彼此可换，故G是一个交换群.

一个群可以分解成为一些互不相交的共轭元素类. 与此相似，群G中所有子群的集合可分成一些互不相交的共轭子群类. 注意，如果K是群G的一个共轭元素类，则K中各个元素的正规化子的集合是G的一个共轭子群类[1].

事实上，如果a和b是K中两个元素，而N_a和N_b分别是这两个元素在群G中的正规化子，则由$b=g^{-1}ag$和$x\in N_a$，即$xa=$ $=ax$，可得出

$$b(g^{-1}xg)=g^{-1}(ax)g=(g^{-1}xg)b,$$

也就是说，

$$g^{-1}N_ag\subset N_b \tag{1}$$

但由$a=gbg^{-1}$用同样的方法可得出

$$gN_bg^{-1}\subset N_a,$$

即

$$N_b\subset g^{-1}N_ag. \tag{2}$$

由(1)和(2)可知

$$N_b=g^{-1}N_ag.$$

现在设有某一子群F和N_a共轭，

$$F=g_1^{-1}N_ag_1,$$

则F将是元素$g_1^{-1}ag_1$的正规化子. 这样一来，我们的定理就被

1) K中两个不相同的元素，其正规化子当然可能相同.

证明了.

现在让我们来证明共轭子群类的一些基本性质.

群 G 中与子群 A 共轭的子群的个数（即这种子群所成集合的势）等于子群 A 的正规化子 N 的指数. 事实上，如同在共轭元素的情形一样，要想用两个不同的元素去作子群 A 的变形而得出同一个与 A 共轭的子群，其充分必要条件是：这两个元素属于 G 对 N 的同一右陪集.

特别，从这里可以看出，所有和子群 A 共轭的子群，其正规化子在群 G 中有相同的指数. 其次，如果 $B=g^{-1}Ag$，则子群 B 的正规化子是 $g^{-1}Ng$. 同时因为映射 $x\to g^{-1}xg$，$x\in N$，是将 N 映到 $g^{-1}Ng$ 上的一个同构映射，且在这样映射下子群 A 被映成子群 B，故 A 在 N 中的指数和 B 在 $g^{-1}Ng$ 中的指数相等. 从这个事实和前面的按语可得出这样一个命题，即子群 A 和 B 在 G 中的指数也相等. 换句话说，*共轭的子群在群中有相同的指数*. 如果这些指数是有限的，则两个共轭的子群之中没有一个子群能够全部包含另一子群. 然而在一般的情形下这却完全是可能的；并且如果 $g^{-1}Ag$ 包含在 A 内且不等于 A，则 $g^{-2}Ag^2$ 将是 $g^{-1}Ag$ 的真子群，$g^{-3}Ag^3$ 将是 $g^{-2}Ag^2$ 的真子群，如此等等. 另一方面，在这样的情形下，A 也是 gAg^{-1} 的真子群，gAg^{-1} 是 g^2Ag^{-2} 的真子群，如此等等.

举例来说，让我们考察全体整数（正的或负的）集合的所有自身相互单值映射所组成的群 G. 我们从这个群中取出由对换

$$(12),\ (23),\cdots,(n,n+1),\cdots,n>0$$

所组成的集合 M，并且用 A 表示由这些对换所生成的子群. 如果 g 表示将 k 映成 $k+1$ 的映射，也就是说，如果采用循环记法时有

$$g=(\cdots,-k,\cdots,-2,-1,0,1,2,\cdots,k,\cdots),$$

则

$$g^{-1}(n,n+1)g=(n+1,n+2),$$

由此即可看出，子群A在群G中和它的真子群——即M中除(12)外所有其余元素所生成的子群——共轭.

群G的一个共轭子群类中所有子群的交是一个正规子群.

事实上，用元素g去作这个共轭子群类中所有子群的变形，我们同时也就作了这些子群的交D的变形. 但用一个元素去作一个共轭子群类中所有子群的变形只不过是将这些子群重排一下，故对群G中的任何一个元素g来说，子群$g^{-1}Dg$永远和子群D相重合. 这就证明了我们的定理. 注意，这个交D当然也可以等于单位子群E.

从这里所证明的定理可得出下面的重要结果:

如果群G中有一个具有限指数的子群，那末在它里面也有一个具有限指数的正规子群.

证明. 如果子群H在G中有有限指数，则如以上所证，所有和H共轭的子群也都是具有限指数的子群. 因为子群H的指数是有限的，故H的正规化子的指数也是有限的，因而和H共轭的子群只有有限个. 如以上所证，这些子群的交是一个正规子群；并且，根据Poincaré定理(§8)，这个交在G中有有限指数.

我们引进一个和正规化子的概念极为相近的概念以结束本节. 如果M是群G中的一个子集，则与M中每一个元素都可换的元素的集合将是群G中的一个子群，这个子群称为集合M在群G中的*中心化子*. 单独一个元素的中心化子和这个元素的正规化子相重合，而在一般情形下集合M的中心化子包含在这个集合的正规化子内. 一个子群的中心化子当然不一定包含这个子群. 群的中心化子即这个群的中心.

显然，集合M的中心化子等于M中各个元素的正规化子的交. 由此不难推出，*群G的一个正规子群的中心化子，或更一般地，群G中任何一个不变集合的中心化子是群G的正规子群.* 事实上，

一个正规子群中所有元素的正规化子组成若干个完整的共轭子群类[1)]，因而这些正规化子的交应该也是一个正规子群. 将这一定理应用于任意子群和它的正规化子，我们可得出：任何一个子群的中心化子是这个子群的正规化子的正规子群。

§ 11a 置换群

在 § 5 里已经证明了，任何一个势为$\mathfrak{M}$的群都与一个势为$\mathfrak{M}$的集到其本身上所有相互单值映射所成的群$S_{\mathfrak{M}}$的一个子群同构. 因此，研究群论只要弄清楚有限对称群和具有无限势$\mathfrak{M}$的群$S_{\mathfrak{M}}$的子群就可以了. 然而，在多数情形，这样做不仅不会给研究提供方便，反而会带来不必要的麻烦. 尽管如此，对称群的子群有时具有这样的用处，描述这些子群在对称群中的状态以及与此相关，这些子群的元素是置换，这些性质起着重要的作用. 其中某些性质将在本节概括地加以叙述.

设给定一个集M. 如同有限集的置换一样，我们把集M到其自身上的相互单值映射叫做集M上一个*置换*. M到其自身上的所有相互单值映射所组成的群的任意一个子群叫做集M上一个*置换群*. 如果M是有限集并且由n个元素组成，那末M上置换群，也就是说，n次对称群的子群，叫做一个*n次置换群*.

设P是集M上一个置换群. 则集M按以下方式被分解成互不相交的类——群P的*传递类*：M的元素a与b属于同一类，当且仅当在P内至少存在一个置换，它将a变成b. a与b之间的这个关系的自反性、对称性和传递性可以由P是群的这个事实直接得出. 显然，集M的每一个在群P的所有置换之下保持不动的元素单独组成一个传递类.

1) 参看本节中所证明的关于共轭元素类和共轭子群类之间的关系的定理.

集M上置换群P说是在M上传递的，如果P只有一个传递类，显然，这个传递类与M重合，换句话说，如果集M的每一个元素都可以通过P的某一个置换变成这个集的任意一个元素．具有多于一个传递类的群叫做非传递群．

设P在集M上是可传递的，又设P_a是P中保持M的一个元素a不动的一切置换所成的集．P_a实际上是P的一个子群．如果P的一个置换σ将元素a变成b，那末右陪集$P_a\sigma$的所有置换都具有这个性质．另一方面，如果P的置换τ也把a变成b，那么乘积$\sigma\tau^{-1}$保持元素a不动，即属于子群P_a，从而τ属于陪集$P_a\sigma$．由群P的传递性，元素a可以变成M的任意一个元素，所以我们得到集M的所有元素与群P关于子群P_a的右陪集之间的一个相互单值对应．如果集M是有限的，也就是说，如果群P是有限的，那末P是有限次置换群．于是子群P_a在群P内的指数是有限的，并且等于群P的次数．这样，根据Lagrange定理，我们得到以下定理：

有限次传递置换群的阶被它的次数整除．

回到一般情形．我们注意，如果P的一个置换σ把元素a变成b，那末等式

$$P_a=\sigma^{-1}P_a\sigma$$

成立．这就是说，在一个传递群P内，对于M的所有元素a，子群P_a是彼此共轭的．它们在群P内构成整个一个共轭子群类．

集M上一个置换群P叫做k重传递的（k是一个自然数），如果集M中元素所成的每一个k元有序组都可以通过P的某一置换变成M中元素的任意另一个k元有序组．这样，n次对称群是n重传递的．n次交错群是$n-2$重传递的．事实上，同时存在两个n次置换，它们都把$n-2$个符号$a_1, a_2, \cdots, a_{n-2}$依次变成$a_{i1}, a_{i2}, \cdots, a_{in-2}$；这两个置换中的一个可以由另一个通过一个对换而得到，因

而其中之一是偶置换．显然，对于 $l<k$，每一个 k 重传递群也是一个 l 重传递群．

集 M 上一个传递置换群 P 说是*非本原的*，如果集 M 可以这样分解成两两不相交的真子集 M_α，其中有一个子集至少含有两个元素（这样的子集 M_α 叫做群 P 的*非本原类*），使得以下要求被满足：如果任意一个非本原类 M_1 中某一元素 a 被 P 的一个置换 σ 变成某一非本原类 M_2 的元素 b，那末 M_1 的每一个元素都被 σ 变成 M_2 中的元素．如果集 M 不能这样分解，那么就说群 P 是*本原的*．

设给出了集 M 被分成关于群 P 的非本原类的一个分解，而 M_1 和 M_2 是其中任意两个非本原类．如果 a_1 和 a_2 分别是 M_1 和 M_2 的元素，那末由群 P 的传递性，在 P 内存在一个置换 σ，它把 a_1 变成 a_2，因而它把 M_1 映成 M_2 的一个子集．实际上，M_1 被映成整个 M_2，因为不然的话，置换 σ^{-1} 将把 M_2 映成一个集合，它包含 M_1 作为真子集，这与非本原类的定义矛盾．特别，由此推出，*所有非本原类 M_α 都具有相同的势*．在有限的情形，这就是说，所有非本原类都含有相同个数的元素．

我们看到，群 P 的每一个置换仅仅置换这些非本原类 M_α，也就是说，引起了这些非本原类所成的集合上的一个置换．显然，类 M_α 所成的集合上一切这样的置换构成一个群，这个群与 P 对于 P 的一个正规子群的商群同构，这个正规子群是由 P 中把 M 的属于每一类 M_α 的元素仍变到 M_α 内的那样的置换组成的．自然，这个正规子群可以仅由一个单位元素构成．

集 M 被分成关于传递群 P 的非本原类的所有分解都可以如下地得到：首先，设 P_a 是由群 P 的所有保持 M 的元素 a 不动的置换所成的子群．如果 Q 是群 P 的一个真子群，并且它包含 P_a 作为真子群，

$$P_a \subset Q \subset P,$$

那末把群 P 分成关于子群 Q 的右陪集. 用 P 关于 Q 的同一右陪集内的置换将 a 变成 M 的某些元素，并且把这些元素都放在一起. 这样就把集 M 分成两两不相交的真子集(因为 $Q \neq P$)，每一个子集至少含有两个元素(因为 $P_a \neq Q$). 容易证明，这是 M 被分成关于群 P 的非本原类的一个分解: P_a 的两个右陪集如果位于 Q 的同一右陪集内，那末同时右乘以 P 的某一元素，仍旧位于 Q 的同一右陪集内.

这样一来，每一个位于 P 与 P_a 之间的子群都给出 M 被分成关于群 P 的非本原类的一个分解. 通过这个方法就可以得出所有这样的分解: 如果给定集 M 的某一个关于群 P 的非本原类的分解，而元素 a 属于非本原类 M_1，那末 P 中所有保持元素 a 仍在 M_1 内的那些置换所成的集 Q 是 P 的一个位于 P 与 P_a 之间的子群，并且不等于这两个群. 集 M 关于子群 Q 的非本原类的分解导致给定的非本原类.

因此，群 P 是本原的当且仅当子群 P_a 是 P 的一个极大真子群. 这时集 M 只可能有平凡分解，即 M 被分成互不相交的子集，这些子集被 P 的元素置换: 即分解成单个的元素，实际上只有 M 本身这一个类.

注意，当 $k>1$ 时，k 重传递群不可能是非本原的. 事实上，如果不然，设元素 a, b 属于同一非本原类，而元素 c 属于另一个非本原类，那末群不可能含有将元素对 a, b 变成元素对 a, c 的置换.

M 的一个真子集 M_0 是传递群 P 的一个非本原类，必要且只要 M_0 至少含有两个元素并且 P 的任意一个置换 σ 如果把 M_0 的一个元素仍旧变到这个子集内，那末 σ 就把 M_0 的每一子集仍映入 M_0 自身内或映到 M_0 自身上.

条件的必要性是明显的. 为了证明这个条件也是充分的，我

们将M的元素如此分类，使得两个符号a与b属于同一类当且仅当存在P的一个置换σ将这两个符号都变到M_0内．集M的这样一个分类的自反性由群P的传递性得出，对称性是显然的．传递性可以这样证明：如果符号a与b经过置换σ变到M_0内，符号b与c经过置换τ变到M_0内，那末符号$b\sigma$属于M_0，从而经过置换$\sigma^{-1}\tau$仍被变到这个子集内．根据M_0的定义，置换$\sigma^{-1}\tau$也把$a\sigma$仍变到M_0内，即$a\tau=(a\sigma)\sigma^{-1}\tau\in M_0$．因此，存在$P$的置换同时将$a$和$c$变到$M_0$内．这样得到的集$M$的分类，其中的一个类就是$M_0$：如果置换$\sigma$将$a$和$b$都变到$M_0$内，而且$a\in M_0$，那末由于

$$a=(a\sigma)\sigma^{-1}\in M_0,$$

根据M_0的定义，将有

$$(b\sigma)\sigma^{-1}\in M_0,$$

即符号b也在M_0内．我们得到所求的集M关于群P的非本原类的分解．

一个本原置换群的任意一个不等于E的正规子群都是传递的．

事实上，设H是集M上置换群P的一个非传递的正规子群，令M_0是关于H的一个传递类，它至少含有两个符号．根据假设，M_0不等于M．如果P的置换σ把M_0中一个符号a仍旧变到M_0内，那末对于H的任意置换τ来说，属于H的置换$\sigma^{-1}\tau\sigma$把符号$a\sigma$变成$a\tau\sigma$，因而仍在M_0内．对于M_0的任意符号b，存在H的一个置换τ_0，使得$b=a\tau_0$，因而$b\sigma$属于M_0．应用上面所证明的定理可知，M_0是关于群P的一个非本原类．

§116 环论基本概念

和群同样作为基本代数理论中研究对象的就是环．环论有着极为丰富的内容，并且已经成为一门巨大的独立学科．环的理论

与本书并没有什么直接的关系．然而，在本书的某些地方有时要用一个环和与它有关的某些概念．在这一节里我们将讨论这些概念和它们的简单性质．

假设在一个用加法书写的阿贝尔群R里，定义第二个代数运算——乘法．R叫做一个环，如果这个乘法关于加法是分配的：

$$a(b+c)=ab+ac,$$
$$(b+c)a=ba+ca.$$

一个环R说是结合的，如果乘法还满足结合律．如果一个结合环R的乘法还满足交换律，就称R是一个结合-交换环，简称交换环．一般说来，今后在环里并不作交换性的假定，然而我们所遇到的环都是结合的．

用来定义环的阿贝尔群叫做环的加法群，这个群的零元素 0 叫做环的零元素．

全体整数关于数的加法和乘法所构成的整数环是最简单的交换环的例子．这个环以后用记号C来表示．矩阵环可以作为非交换的结合环的例子：如果取元素是整数(或者，例如，元素是实数)的全体n阶方阵所成的集合，保留通常矩阵乘法的定义，而两个矩阵的和是这样一个矩阵，它的元素是由所给的矩阵对应位置的元素相加而得到的．容易验证，这是一个环．

环R_1与R_2说是同构的，如果存在第一个环的加法群到第二个环的加法群上一个同构映射，并且在这个映射之下，R_1的两个元素的乘积被映成R_2中对应元素的乘积．在环的一般理论里，同构的环不认为是不同的．

由环的定义得到等式

$$a\cdot 0=0\cdot a=0,$$

这里a是环的任意元素．事实上，$a\cdot 0=a(0+0)=a\cdot 0+a\cdot 0$，于是由环的加法群中减法的单值性得$a\cdot 0=0$．

然而，如果环的两个元素的乘积等于零，$ab=0$，一般来说，并不能断言其中一个因子等于零．例如，在矩阵环里，元素

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

不等于零，而它们的乘积等于零．环中不等于零的元素，而它们的乘积等于零，叫做*零因子*．如果在一个环里，有的元素是零因子，那末就称这样的环为*带零因子的环*．带零因子的交换环的例子将在下面给出．

环R的元素e叫做这个环的*单位元*，如果对于R的任意元素a，都有

$$ae=ea=a.$$

偶数环的例子告诉我们，并不是所有的环都有单位元．

一个有单位元e的交换环叫做一个*域*，如果这个环含有非零元素，并且每一个非零元素a都有一个逆元a^{-1}，满足条件

$$aa^{-1}=e.$$

域没有零因子，因为如果$ab=0$而$b\neq 0$，那末乘以b^{-1}就得$a=0$．这样，一个域的所有不等于零的元素对于乘法作成一个阿贝尔群——*域的乘法群*．有理数域，实数域和复数域都是域的例子．

环R的一个子集R'叫做R的一个*子环*，如果它对于环R的运算来说，本身也作成一个环．子环R'的加法群显然是环R的加法群的一个子群．

环R的子环A叫做R的一个*左理想*，如果它容许R的元素从左边去乘，也就是说，如果对于A的任意元素a和R的任意元素r，乘积ra属于A．类似地可以定义*右理想*和*双侧理想*．显然，在交换环的情形，就可以简单地称为*理想*．一个环本身和只由单独一个零元所组成的*零理想*都是这个环的双侧理想．

环R的任意一组左(或右或双侧)理想的交仍是这个环的左(或右或双侧)理想. 两个理想A与B的交记作$A\cap B$.

设在环R里，给定两个左理想A和B. 考虑这两个理想的加法群的和. 这个和由一切形如$a+b$的元素组成，这里$a\in A, b\in B$. 如果r是R的任意一个元素，那末

$$r(a+b)=ra+rb.$$

因为$ra\in A, rb\in B$，所以$r(a+b)$属于这个和. 这就证明了，左理想A与B的和仍是环R的一个左理想. 左理想的这个和记作(A, B). 类似地可定义右(或双侧)理想的和.

如果给定环R的一个双侧理想D，那末在环R的加法群关于子群D的商群R/D里，可以如下地定义乘法：陪集$a+D$与$b+D$的乘积定义为陪集$ab+D$. 这个乘积不依赖于元素a与b在各自所在的陪集内的选取：如果

$$a'=a+d_1,\quad b'=b+d_2,\quad d_1, d_2\in D,$$

那末

$$a'b'=ab+(ad_2+d_1b+d_1d_2),$$

其中括号里面的表示式属于D. 容易验证，商群R/D对于这样定义的乘法来说作成一个环. 这个环叫做环R关于理想D的商环.

例如，在整数环C里，能被n整除的全体整数的集合是一个理想. 事实上，两个能被n整除的整数的差以及能被n整除的整数与任意一个整数的乘积仍可被n整除. 环C关于这个理想的商环记作C_n. 这个环是有限的，它的加法群是一个n阶循环群. 如果n是一个合数，则C_n有零因子. 事实上，如果$n=pq$，那末p和q所生成的类都不等于零类，而它们的乘积等于零类，即数n所生成的理想. 如果n是一个素数，那末容易证明，环C_n不但没有零因子，而且还是一个域.

与主理想环有关的某些环论的结果将在§22a里补充给出。例如，环R的一个左理想A叫做一个主理想，如果在A中可以找到这样一个元素a，使得A与R中一切含有元素a的左理想的交重合。

第四章 自同态与自同构·带运算子的群

§12. 自同态与自同构

凡将群G映入其自身,即映到它的一个子群上的同态映射,叫做这个群的*自同态*. 群的自同态中的一种就是*自同构*, 即将群映到它自身上的同构映射. 自同构的一个明显的例子就是将群映到它自身的恒等映射. 也就是所谓*恒等自同构*;在这个自同构下,群的每一个元素都保持不变. 对整数加法群的映射, 将每个整数n映成整数$-n$的,就是一个非恒等自同构的例子.

任何一个群都具有一个*零自同态*, 这个自同态将群中每一个元素都映成它的单位元. 在群的其他的自同态中也可能存在这样的一些,它们虽然不是自同构,可是却将群映到它自身上. 这种情况在群和其一个真商群同构时就会出现,因而这种群必是无限群,在§10中我们已指出存在这种群. 一个群和它的一个子群之间的任何一个同构也是这群的一个自同态. 不是自同构的这样一种自同态的例子可在整数加法群中找到.

在群G的一个自同态之下, 它的每一个子群H都受到一个同态映射,而在一个自同构之下子群H所受到的将是一个同构映射. 由此可知, 子群H在群G的自同态(自同构)χ之下的象也是这个群的一个子群,这个子群记作$H\chi$. 这样,群G本身在自同态χ之下的象就是$G\chi$.

如果群G是由生成系$M=\{a_\alpha\}$所给出的, 那末这个群的任何一个自同态χ,在指出所有生成元的象$a_\alpha\chi$之后, 即可完全决定. 特别是,如果χ是群G的一个自同构,则M中所有元素在自同构χ之下的象的集合也是群G的一个生成系.

设已从群G中选出某一元素a，则将这个群的每一元素x映成元素$a^{-1}xa$的映射(即整个群G经元素a的变形)是群G的一个自同构. 事实上,由$a^{-1}xa=a^{-1}ya$可得出$x=y$,也就是说,这个映射是相互单值的. 等式

$$x=a^{-1}(axa^{-1})a$$

表明,在这个映射下群G中的每个元素都是某一元素的象.最后,由

$$a^{-1}xa\cdot a^{-1}ya=a^{-1}(xy)a$$

可知所讨论的映射是一个同构映射. 群G的这样一种自同构称为它的内自同构. 所有不是内自同构的自同构都称为外自同构. 恒等自同构是内自同构之一——可以把它看作是用单位元去作群的变形得出的自同构. 对阿贝尔群的情形，这是唯一的内自同构. 在一般情形下,要元素a所引出的内自同构是恒等自同构,其充分必要条件是元素a属于群的中心,因为等式

$$a^{-1}xa=x$$

对群G中所有元素x成立这一条件，等价于元素a与群G中所有元素x可换.

在群的一个内自同构下,每一个共轭元素类都被映成它自身. 但也存在具有同样性质的外自同构的群,并且是有限群.

二阶循环群只有一个自同构,即恒等自同构. 可是,这个群是唯一的除恒等自同构外不再具有其他自同构的群. 事实上，任何一个非交换群必定具有非恒等内自同构. 其次，如果G是一个阿贝尔群,并且除单位元外还有阶$\neq 2$的元素，则将这个群的每一个元素a映成其逆元素a^{-1}的映射是一个非恒等自同构，因为由于运算是可换的,等式

$$(ab)^{-1}=a^{-1}b^{-1}$$

成立. 最后，对于那些只具二阶元素的非循环的阿贝尔群，由它们的结构的完全描述可知它们具有非恒等自同构，这一描述将在

§ 24 中给出.

自同构群 群 G 的自同态是这个群的自身映射中的一种. 因此,我们可以在相继施行自同态的意义下来谈自同态的乘法:设已知群 G 的两个自同态 χ 和 η, 那末他们的乘积 $\chi\eta$ 是这样一个映射,对 G 中任意元素 a

$$a(\chi\eta)=(a\chi)\eta.$$

自同态的乘积还是自同态. 事实上

$$(ab)(\chi\eta)=[(ab)\chi]\eta=(a\chi\cdot b\chi)\eta=(a\chi)\eta\cdot(b\chi)\eta=$$
$$=a(\chi\eta)\cdot b(\chi\eta).$$

显然,在这样的定义下自同构乘积也还是自同构.

由 § 1 中的结果可知,自同态的乘法满足结合律, 在上面所引入的恒等自同构则起着单位元的作用. 可是我们却不能认为群 G 的自同态对这样定义的乘法组成一个群, 因为在一个同态映射下原像不是唯一的,故不能对每个自同态都定义它的逆映射. 显然,只有自同构才具有逆映射,并且这些逆映射同样也是自同构.

我们看到,群 G 的所有自同构的集合 Φ 也是一个群,群 G 的这个自同构群是所有将 G 映成其自身的相互单值映射所组成的群 $S(G)$ 的子群.

群 G 的内自同构是其所有自同构的群中的一个子群, 因为相继以元素 a 和 b 去作群 G 的变形和用元素 ab 去作它的变形是等效的. 此外,如果对群 G 的每个元素,使由这个元素所引出的内自同构和它相对应,我们就得出一个同态映射,将群 G 映到它的内自同构群 Φ' 上. 正如上面已经指出的,在这个同态映射下被映成群 Φ' 的单位元的,是而且只能是群 G 的中心 Z 中的元素. 这就是说,群 G 的内自同构群和群 G 对其中心 Z 的商群同构:

$$\Phi'\simeq\frac{G}{Z}.$$

特别，从这里还可以看出，群G中两个元素a和b引出同一内自同构的充分必要条件是：a和b包含在群G对其中心Z的同一陪集内.

内自同构群是所有自同构所组成的群的一个正规子群。事实上，设已知群G的一个自同构φ和由元素a所引出的一个内自同构α. 于是对群G中任意元素x有

$$x(\varphi^{-1}\alpha\varphi)=[a^{-1}(x\varphi^{-1})a]\varphi=(a^{-1})\varphi\cdot(x\varphi^{-1})\varphi\cdot a\varphi=$$
$$=(a\varphi)^{-1}\cdot x\cdot(a\varphi),$$

也就是说，自同构$\varphi^{-1}\alpha\varphi$是由元素$a\varphi$所引出的内自同构.

要定出一个已知的群G的自同构群，一般是非常困难的. 在大多数情形下，群G本身的性质不能转移到它的自同构群上去. 举例说，一个阿贝尔群的自同构群就可能是一个非交换群，例如我们在§9中所遇到的4阶非循环阿贝尔群，其自同构群就是3次对称群. 另一方面，也存在这样的非交换群，它的自同构群是阿贝尔群. 但一个非交换群G的自同构群却不可能是循环群，因为G的内自同构群和G对其中心的商群同构，因而不可能是循环群(§11)，而一个循环群的子群必定是循环群(§6).

显然可以断定，一个n阶有限群的自同构群一定也是一个有限群. 这个群是n次对称群的一个子群，因而它的阶是整数$n!$的一个约数. 事实上，这个群的阶甚至还是整数$(n-1)!$的约数，因为群中的单位元在所有自同构下都保持不变. 关于有限群的自同构群的阶更精确的上界，可在Birkhoff和Hall的论文[1]及Ляпин的论文[1]中找到.

无限群的自同构群也可能是有限群，例如：在无限循环群中只有两种方法可以选择生成元素；但因为循环群中一个元素是生成元素的性质在自同构下保持不变，故无限循环群的自同构群是一个2阶循环群. 正有理数乘法群的自同构群具有连续统的势，因

为任意一个将所有素数的集合映到它自身上的相互单值的映射都能引出这个群的一个自同构.

互不同构的群，其自同构群可能同构. 例如，在上面已经指出，无限循环群的自同构群是一个 2 阶循环群；但很容易看出，3 阶循环群的自同构群也是 2 阶循环群. 另一面，也存在这样的群，它们不是任何群的自同构群. 例如：奇数阶的有限循环群就是这样的群. 正如上面所说过的那样，这样的群不可能是非交换群的自同构群. 而对于不是 2 阶循环群的阿贝尔群来说，它们的自同构群中必定含有 2 阶的元素，因此，如果这些自同构群是有限群，则他们的阶必定是偶数.

中心的不存在是群的性质中对自同构群仍旧保持不变的性质之一：

如果群 G 是一个无中心群，则它的自同构群 Φ 也是无中心群.

事实上，设 φ 是群 G 的一个自同构，但不是恒等自同构；设 a 是 G 的这样一个元素，它适合条件 $a\varphi=a'\neq a$，如果自同构 φ 属于群 Φ 的中心，则 φ 必定与由元素 a 所引出的群 G 的内自同构可换，也就是说，对群 G 的任意元素 g，

$$a^{-1}(g\varphi)a=(a^{-1}ga)\varphi=a'^{-1}(g\varphi)a'.$$

但 $g\varphi$ 和元素 g 一起遍历整个群 G，故元素 a 和 a' 引出群 G 的同一内自同构；然而这是和 G 是无中心群这一假定相违的. [参看补充 3.1 和 § 补充 22.]

§ 13. 全形 · 完全群

用群 G 中一个元素 a 去作这个群的变形时，G 的每个子群 H 被变成和它共轭的子群 $a^{-1}Ha$(参看 § 9)，因而每个正规子群都被映成其自身. 正规子群在群的所有内自同构下不变的这一性质，可以用来作为正规子群的另一定义. 用群 G 中一个元素去作 G 的变

形时，G的正规子群H所受到的那个映到自身上的映射是H的一个自同构，但一般说来已经不是一个内自同构了．换句话说，如果一个群是另一群的正规子群，则大群的内自同构引出小群的自同构．现在就产生了一个问题，能不能将一个任意的已知群G作为一个正规子群嵌入另一群内，使得G的全部自同构都能从这个大群的内自同构导出？用下面的方法可以得出这个问题的一个肯定的解答．

在§5中已经证明，如果对群G中每个元素a，使将群G中每个元素x映成元素xa的映射和它相对应，我们就可以得出一个同构映射，它将群G映到由群G的全部到自身相互单值映射所组成的群$S(G)$．按照这一方法，群$S(G)$中由群G同构地映成的子群$\bar{G}$可以看作和群G完全相同．但在这里群G中的元素作为被置换的符号和作为群$S(G)$中的元素必须予以区别，因此我们用$\bar{a}$来表示群$\bar{G}$中和群G中的元素a相对应的元素．

子群$\bar{G}$在群$S(G)$中的正规化子Γ称为群G的全形．从正规化子的定义可知，群Γ包含$\bar{G}$作为其正规子群．现在我们要证明，群$\bar{G}$的所有自同构都能由群Γ的内自同构导出．

我们知道，群G的自同构群Φ是群$S(G)$的子群，现在让我们证明群Φ包含在群Γ内，也就是说，证明群G的任何一个自同构φ，被看作群$S(G)$中的一个元素时，都和子群$\bar{G}$可换．设$\bar{a}$是$\bar{G}$中任一元素，现在让我们来看一看乘积$\varphi^{-1}\bar{a}\varphi$是群$G$的怎样一个映射．在自同构$\varphi^{-1}$下$G$的元素$x$被映成元素$x\varphi^{-1}$，映射$\bar{a}$将这个元素变成乘积$x\varphi^{-1}\cdot a$，而自同构$\varphi$则给出

$$(x\varphi^{-1}\cdot a)\varphi=(x\varphi^{-1})\varphi\cdot a\varphi=x\cdot a\varphi;$$

这样我们就看到，乘积$\varphi^{-1}\bar{a}\varphi$和子群$\bar{G}$中的元素$\overline{a\varphi}$相重合．这就证明了自同构$\varphi$包含在全形$\Gamma$内。

与此同时，如果命$\bar{a}$遍历子群$\bar{G}$中所有的元素，我们还可以看

出：用元素φ去作$\bar{G}$的变形，即可得出$\bar{G}$中的一个映射，且这个映射和群G的自同构φ相重合．这就是说，群$\bar{G}$所有的自同构都能由全形Γ的内自同构引出[1)]．

现在让我们来求出群$\bar{G}$在群$S(G)$中的中心化子Z．设映射ζ属于Z，也就是说，对$\bar{G}$中的任意元素$\bar{a}$，

$$\bar{a}\zeta=\zeta\bar{a}, \tag{1}$$

群G中的单位元在映射ζ下的像是群G中的一个元素，这个元素我们将方便地记作s^{-1}，

$$1\zeta=s^{-1}.$$

因为

$$1(\bar{a}\zeta)=(1\cdot a)\zeta=a\zeta,$$

$$1(\zeta\bar{a})=(s^{-1})\bar{a}=s^{-1}a,$$

故由(1)可知

$$a\zeta=s^{-1}a \tag{2}$$

对所有a成立．

反之，对G中任意元素s，由等式(2)所定义的，将群G映成其自身的映射ζ属于Z．事实上，这个映射的相互单值性是很明显的．如果b是G中一个任意元素，则

$$a(\bar{b}\zeta)=(ab)\zeta=s^{-1}(ab),$$

$$a(\zeta\bar{b})=(a\zeta)b=(s^{-1}a)b,$$

也就是说，$\bar{b}\zeta=\zeta\bar{b}$．

因此，对于G中一切可能的s，(2)这种形式的映射就穷尽了Z中的全部元素．在这里，和不同元素s相当的映射ζ也彼此不同，也就是说，群G和Z之间的这一对应是一个相互单值的对应，这个对应甚至还是一个同构对应：如果ζ和η是Z中两个元素，s和t

1）这个结果给出了前面所提问题的解答．如果读者不愿意讨论群$\bar{G}$，而愿意讨论原来的群G，那末可以在集合Γ中用G的元素来替换$\bar{G}$中相应的元素，并且将群Γ中的运算推移到这个新得出的集合上来．

是G中和它们相对应的元素，即对G中任意元素a

$$a\zeta=s^{-1}a,\ a\eta=t^{-1}a,$$

则

$$a(\zeta\eta)=(a\zeta)\eta=(s^{-1}a)\eta=t^{-1}s^{-1}a=(st)^{-1}a.$$

子群Z包含在群G的全形Γ内，并且，如在§11末所记，还是它里面的一个正规子群. 另一方面，$\bar{G}$也是Γ的正规子群. 因此

$$\{Z,\bar{G}\}=Z\bar{G}.$$

群G的内自同构群Φ'整个地包含在群Γ的子群$Z\bar{G}$内. 事实上，明显的等式

$$s^{-1}as=(s^{-1}a)s \tag{3}$$

表明，以元素s去作群G变形所得出的映射，当作$S(G)$中的一个元素看待时，等于Z中与元素s相对应的元素和$\bar{G}$中元素$\bar{s}$的乘积. 由等式(3)还可以看出，*子群Z包含在群Φ'和$\bar{G}$的乘积内，*因此

$$Z\bar{G}=\Phi'\bar{G} \tag{4}$$

全形Γ是群$S(G)$中的子群Φ和$\bar{G}$的乘积，

$$\Gamma=\Phi\bar{G}.$$

事实上，设τ是Γ中一个任意的元素. 由于这个元素和$\bar{G}$可换，故用元素τ去作$\bar{G}$的变形可得出$\bar{G}$的一个自同构；根据上面所证，这个自同构也可以用Φ中的一个元素φ去作$\bar{G}$的变形而得出. 因此，元素$\tau\varphi^{-1}$和群$\bar{G}$中的每个元素可换，也就是说，$\tau\varphi^{-1}$属于子集Z，根据(4)，它又属于乘积$\Phi'\bar{G}$. 因此，元素τ包含在乘积$(\Phi'\bar{G})\Phi=\Phi\bar{G}$内. [参看补充 3.2.]

完全群 如果群G是一个无中心群，并且它的每一个自同构都是内自同构，则G称为*完全群*. 因此，完全群和它的自同构群相重合. 下面的定理(Hölder[2])给出完全群的一些重要的例子.

如果$n\geqslant 3, n\neq 6$，则有限对称群S_n是一个完全群.

证明. 在 $n \geqslant 3$ 时群 S_n 显然是一个无中心群. 现在让我们来考察这个群的自同构. 首先注意, S_n 中的 2 阶元素是, 而且仅仅是那些能够分解成为一些两两不相交的对换乘积的置换. 设

$$a=(a_1a_2)(a_3a_4)\cdots(a_{2k-1}a_{2k}),\quad 2\leqslant 2k\leqslant n,$$

是这样的元素中的一个(所有 $a_i, i=1,2,\cdots,2k$, 都彼此不同). 我们证明: 元素 a 在群 S_n 中的共轭元素系由所有能够分解成为 k 个彼此不相交对换乘积的置换组成.

事实上, 如果

$$b=(\beta_1\beta_2)(\beta_3\beta_4)\cdots(\beta_{2k-1}\beta_{2k})$$

是这样的置换中的一个(这里所有 $\beta_i, i=1,2,\cdots,2k$, 也是互不相同的), 则 b 可由元素 a 经过任意一个形式如

$$\begin{pmatrix}\alpha_1\alpha_2\cdots\alpha_{2k}\cdots\\ \beta_1\beta_2\cdots\beta_{2k}\cdots\end{pmatrix}\tag{5}$$

的置换变形得出. 反过来, S_n 中的任意一个置换都可以写成(5)这种形式, 因而用这个置换去作 a 的变形时, 就得到是一个形式如 b 的元素.

我们用 C_k 表示由所有能够写成 k 个彼此不相交的对换的乘积的 2-阶元素所组成的共轭元素类. 特别地, C_1 由一切对换 $(\alpha_1\alpha_2)$ 所组成.

群的任意一个自同构都使元素的阶保持不变, 且将每个共轭元素类映成另一完整的共轭元素类. 因此, 如果 φ 是群 S_n 的一个任意的自同构, 则它应该将共轭元素类 C_1 映成某一共轭元素类 $C_k, k\geqslant 1$. 我们证明: 如果 $n\neq 6$, 则在自同构 φ 之下共轭元素类 C_1 只能被映成其自身.

对于 $n=3$ 的情形这是很明显的, 因为在这时群 S_3 中所有 2-阶元素都包含在 C_1 内. 设 $n\geqslant 4$, 共轭元素类 C_1 由

$$\frac{n(n-1)}{2} \tag{6}$$

个不同的元素组成. 如果 $k\geqslant 2$, 则由所有形式如

$$(\alpha_1\alpha_2)(\alpha_3\alpha_4)\cdots(\alpha_{2k-1}\alpha_{2k})$$

的元素所组成的集合 C_k 共包含

$$\frac{n(n-1)\cdots(n-2k+2)(n-2k+1)}{k!\,2^k} \tag{7}$$

个元素: 分母里出现整数 2^k 是因为在每个对换里符号的位置可以互换; 而整数 $k!$ 的出现, 则是因为这 k 个对换本身可以任意排列. 如果在自同构 φ 之下, 共轭元素类 C_1 被映成 C_k, $k\geqslant 2$, 那末这两个共轭元素类应该由同样个数的元素组成. 命(6)和(7)相等, 我们得出等式

$$(n-2)(n-3)\cdots(n-2k+2)(n-2k+1)=k!\,2^{k-1}. \tag{8}$$

因为 $n\geqslant 2k$, 故在 $k=2$ 时这个等式不论对怎样一个整数 n 都不能成立. 在 $k=3$ 时, 如果 $n=6$, 这个等式是可以成立的. 如果 $k\geqslant 4$, 则等式(8)的左端永远大于它的右端. ——只要对使得等式左端取最小值 $n=2k$ 时来验证这一点就够了.

在下面我们假定 $n\neq 6$, *如果 α 是被置换的符号之一, 则必存在一个符号 α', 使所有含 α 的对换在自同构 φ 下被映成所有含 α' 的对换.*

事实上, 在上面已经证明, 一个对换在 φ 之下的象还是一个对换. 如果

$$(\alpha\beta)\varphi=(\beta'\beta''),$$
$$(\alpha\gamma)\varphi=(\gamma'\gamma''),$$

且符号 $\beta',\beta'',\gamma',\gamma''$ 互不相同, 则对换 $(\alpha\beta)$ 和 $(\alpha\gamma)$ 的乘积将是一个 3 阶元素 $(\alpha\beta\gamma)$, 而他们的象的乘积则是一个 2 阶元素. 这就证明了我们的断语在 $n=3$ 时是正确的.

如果 $n\geqslant 4$, 则可能出现这样的情形, 即:

$$(\alpha\beta)\varphi=(\alpha'\beta'),$$
$$(\alpha\gamma)\varphi=(\alpha'\gamma'),$$
$$(\alpha\delta)\varphi=(\beta'\gamma').$$

但在这时乘积

$$(\alpha\beta)(\alpha\delta)(\alpha\gamma)=(\alpha\beta\delta\gamma)$$

的阶是 4，而象的乘积

$$(\alpha'\beta')(\beta'\gamma')(\alpha'\gamma')=(\beta'\gamma')$$

的阶则等于 2. 这样我们就证明了：对于已知的符号 α，所有$(\alpha\beta)$这种形式的对换在自同构 φ 之下的象都含有一个共同的符号 α'. 这些象就是含有符号 α' 的全部对换，因为不然的话，在逆映射 φ^{-1} 下将会导致与已得结果相矛盾的结果.

这样一来，映射 $\alpha\to\alpha'$ 就是所有被置换的符号的集合的一个相互单值自身映射，也就是说，是群 S_n 中的一个置换. 我们用 s 来表示这个置换，

$$\alpha'=\alpha s$$

现在如果$(\alpha\beta)$是一个任意的对换，则它在自同构 φ 之下的象应该是一个既包含符号 αs 也包含符号 βs 的对换，即

$$(\alpha\beta)\varphi=(\alpha s,\beta s).$$

但这个式子的右端刚好就是对换$(\alpha\beta)$经过置换 s 变形后的象，因此，自同构 φ 和由元素 s 所引出的内自同构对于一切对换，因而对于群 S_n 的一切元素(因为我们知道，S_n 中的元素都是对换的乘积)所起的作用一致. 定理证完.

在 Schreier 和 Ulam 的论文[3]中证明了：对于任意无限集合 M，所有将 M 映成其自身的相互单值映射，其所组成的群 S_M 是一个完全群. 在 Гольфанд 讨论某些群的全形的自同构的论文[3]中，可找到完全群的一些例子. [参看补充 3.2.]

§14. 特征子群与全特征子群

设 a 和 b 是群 G 的两个元素. 如果可以找到群 G 的一个自同构 φ 将 a 映成 b:

$$a\varphi=b,$$

则 a 和 b 称为同型元素. 同型元素显然有相同的阶. 整个群 G 可以分解成为一些互不相交的同型元素类, 其中每一个同型元素类都是群 G 的不变集合. 群 G 的一个同型元素类是 G 的全形中一个共轭元素类. 利用这一点就可以将 §11中所得出的有关共轭元素类的许多结果推移到同型元素类上来.

按同一方式可以定义群 G 的同型子群和同型子群类. 同型的子群必定同构且有相同的指数: 如果子群 A, B 和自同构 φ 适合关系 $A\varphi=B$, 则对 G 中任意元素 g, 陪集 Ag 在自同构 φ 下被映成陪集 $B(g\varphi)$; 但因为 $g\varphi$ 是群 G 中任意的元素, 故利用这一事实可在群 G 对子群 A 和 B 的右陪集之间建立起一个相互单值对应. 上面的断语同样也可以由这样一个事实推出, 即群 G 的同型子群类是 G 的全形中的共轭子群类.

正如在前面我们把和所有共轭子群相重合的一类子群, 即正规子群划分了出来一样, 现在我们也可以把和所有同型子群相重合的子群, 即在群的所有自同构下都被映成其自身的子群特别划分出来. 这样的子群称为特征子群.

群 G 的特征子群 H 是任何一个包含 G 作为正规子群的群 $\bar{G}$ 的正规子群. 事实上, 群 $\bar{G}$ 的每个内自同构引出群 G 的一个自同构, 因而将子群 H 映成其自身. 反过来, 由全形的定义可知, 如果群 G 的子群 H 是 G 的全形的正规子群, 那末它就是 G 的特征子群.

如果群 G 的子群 H 在群 G 所有自同态 χ 下被映入其自身(即映到其自身上或映到 H 的一个子群上):

$$H\chi\subseteq H,$$

则H称为全特征子群(或全不变子群). 全特征子群对自同态的关系犹如特征子群对自同构的关系，正规子群对内自同构的关系.

每个全特征子群都是特征子群.

事实上，如果子群A是群G的全特征子群，则在群G的所有自同构下它都被映入自身. 如果在某一自同构φ之下，子群A被映成它自己的一个真子群，则在自同构φ^{-1}下它将被映成一个比它大的子群. 然而这是和我们的假定相违的.

一个群是另一群的正规子群这个性质不是可传的，而一个子群是特征子群或全特征子群这一性质却是可传的：*如果群A是群B的特征子群(全特征子群)，而B是群C的特征子群(全特征子群)，则A也是C的特征子群(全特征子群).* 事实上，群C的每一个自同构(自同态)都同构(同态)地将群B映成(入)其自身，因而也将群A同构(同态)地映成(入)其自身.

另一方面，还要指出，如果

$$A\subset B\subset C,$$

且A是C的特征(全特征)子群，此时A却不见得是B的特征(全特征)子群.

群G中任意一组特征(全特征)子群的交，以及由这一组子群所生成的子群也是群G的特征(全特征)子群.

这两个断语中的第一个是很明显的. 第二个断语可以证明如下：设已知一组全特征子群A_α(α遍历某一个足标)，并设这一组子群所生成的子群是B. 子群B的任意元素b具有形式：

$$b=a_{\alpha_1}a_{\alpha_2}\cdots a_{\alpha_k}\quad a_{\alpha_i}\in A_{\alpha_i}.$$

如果χ是群G的任意一个自同态，则

$$b\chi=a_{\alpha_1}\chi\cdot a_{\alpha_2}\chi\cdots a_{\alpha_k}\chi,$$

但由$a_{\alpha_i}\chi\in A_{\alpha_i}$即可得出$b\chi\in B$. 如果$A_\alpha$是特征子群，$\chi$是群$G$的

一个任意的自同构，那么我们也同样可得出 $B\chi\subseteq B$，如果在这里严格的包含关系 $B\chi\subset B$ 成立，则在逆映射 χ^{-1} 下子群 B 将被映成一个比它大的子群. 因此，$B\chi=B$，

每一个群本身和它的单位子群都是它自己的全特征子群，因而也是它的特征子群. 除此二者之外不再具有其他特征子群的群称为*初等群*. 所有单纯群显然都是初等群. 我们已经多次遇到过的 4 阶非循环群也是初等群. [参看补充 3.2.]

循环群的所有子群都是全特征子群.

事实上，如果在自同态 χ 下这个群的生成元 a 被映成 a^k：$a\chi=a^k$，则

$$(a^s)\chi=(a\chi)^s=a^{ks},$$

也就是说元素 a^s 所生成的循环子群将被映入其自身.

一个群的中心是它的一个特征子群，因为一个和群中所有元素可换的元素，在自同构下的像也具有同样性质，如果对 G 中所有元素 x 有

$$ax=xa,$$

则对任意自同构 φ 有

$$a\varphi\cdot x\varphi=x\varphi\cdot a\varphi.$$

元素 $x\varphi$ 和元素 x 一道遍历整个群 G.

然而我们必须特别注意：*群的中心不一定是它的全特征子群.* 举例来说，让我们看一看有理数域上的满秩 2 阶矩阵的群. 如果 a 是一个这样的矩阵，则它的行列式是一个不等于零的有理数，因而可以写成 $\frac{s}{t}2^{n(a)}$ 这种形式，其中 s 和 t 都是奇数，而整数 $n(a)$ 则可能大于，等于或小于零. 因为矩阵乘积的行列式等于他们的行列式的乘积，故我们可得出等式

$$n(ab)=n(a)+n(b),$$

对G中的每个矩阵a，我们使矩阵(也包含在G内)

$$a\varphi=\begin{pmatrix}1 & n(a)\\0 & 1\end{pmatrix}$$

和它相对应，我们得到一个将G映入其自身的映射φ，等式

$$(ab)\varphi=\begin{pmatrix}1 & n(ab)\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & n(a)+n(b)\\0 & 1\end{pmatrix}=$$

$$=\begin{pmatrix}1 & n(a)\\0 & 1\end{pmatrix}\begin{pmatrix}1 & n(b)\\0 & 1\end{pmatrix}=a\varphi\cdot b\varphi$$

说明，映射φ是群G的一个自同态. 然而

$$\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}\varphi=\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix},$$

也就是说，一个属于群G的中心的矩阵被φ映成一个不属于中心的矩阵.

作为任意群G的全特征子群的例子，我们可以举出当n为某一自然数时G中所有元素的n次幂所生成的子群，以及所有有限阶元素所生成的子群. 事实上，在任何一个自同态下，元素a的n次幂的象即这个元素的象的n次幂，而每个有限阶元素都被映成有限阶元素.

换位元　全特征子群的一个十分重要的例子和下面的概念有关，这概念本身也有着非常重要的意义：如果已知任意一个群G中两个元素a和b，则G中的元素

$$[a,b]=a^{-1}b^{-1}ab$$

称为这两个元素的*换位元*. 换位元等于单位元的充分必要条件是元素a和b可换；而在一般的情形下则这个元素在某种意义上标志a和b的可换性，因为我们有：

$$ab=ba\cdot[a,b].$$

换位元的下列性质可由直接的计算来验证（a, b, c是群中任

意元素):

$$[a,b][b,a]=1. \text{ 从而 } [a,b]^{-1}=[b,a], \tag{1}$$

$$[a,b^{-1}]=b[b,a]b^{-1}, [a^{-1},b]=a[b,a]a^{-1}, \tag{2}$$

$$[ab,c]=b^{-1}[a,c]b[b,c], \tag{3}$$

$$[a,bc]=[a,c]c^{-1}[a,b]c. \tag{4}$$

求换位元的运算可以看作是在群元素的集合中定义的一个新运算. 在一般的情形,这个运算不适合结合律,也就是说,等式:

$$[[a,b],c]=[a,[b,c]] \tag{5}$$

不是永远成立的. 为了回答在怎样的条件下群 G 中等式(5)成立的问题,我们定义下面一类范围较阿贝尔群为广的群.

如果群 G 中任意两个元素的换位元都包含在中心内,则 G 称为亚阿贝尔群[1].

在第十五章中我们还要讨论亚阿贝尔群. 下面的两个定理(Levi[6])能说明亚阿贝尔群和求换位元运算之间的关系.

I. 在亚阿贝尔群中,并且只有在这一类群中,求换位元的运算满足结合律.

事实上,在一个亚阿贝尔群中等式(5)永远能够满足,因为这个等式的两端都等于单位元. 反之,设在群 G 中等式(5)对任意 a, b 和 c 成立. 命 $c=b$, 我们可得出

$$[[a,b],b]=1;$$

从这个等式由(2)和(1)可得出

$$[a,b]^{-1}=[a,b^{-1}]. \tag{6}$$

因为 a 和 b 是任意的元素,故在(6)中我们可分别用 b 和 a^{-1} 来代替他们,然后运用(1). 这样我们就得出

$$[a,b]^{-1}=[a^{-1},b]. \tag{7}$$

1) 现在把这种群叫做第二类幂零群更合适些. [参看补充 24.4.]

最后，由等式(6)和(7)可得出

$$[a,b]=[a^{-1},b^{-1}]. \tag{8}$$

现在我们重新把 a,b 和 c 看作任意的元素，并利用公式(6)，(7)，(8)和(1)作等式(5)两端的变形：

$$[[a,b],c]=[[a,b]^{-1},c^{-1}]=[a,b]c[a,b]^{-1}c^{-1}=$$
$$=[a^{-1},b^{-1}]c[a^{-1},b]c^{-1};$$
$$[a,[b,c]]=[a^{-1},[b,c]^{-1}]=a[b,c]a^{-1}[b,c]^{-1}=$$
$$=a[c^{-1},b]a^{-1}[b,c^{-1}],$$

命所得的结果相等，经过简单的变形后可得出等式

$$ba^{-1}b^{-1}cab^{-1}a^{-1}c^{-1}bab^{-1}cbc^{-1}=1,$$

由此即得出

$$[b^{-1}c,a]b^{-1}[a,b^{-1}c]b=1$$

或由(1)，

$$[[a,b^{-1}c],b]=1,$$

但元素 $a,b^{-1}c,c$ 和元素 a,b,c 一样，都是群 G 中的任意元素，所以我们就证明了群 G 任意两个元素的换位元和 G 中任意元素可换，也就是说，G 是一个亚阿贝尔群.

II. 在亚阿贝尔群中，并且只有在这一类群中，求换位元的运算与群中的乘法由两个分配律联系着即

$$[ab,c]=[a,c][b,c], \tag{3'}$$
$$[a,bc]=[a,b][a,c]. \tag{4'}$$

事实上，等式(3)和(3′)的右端相等的充分必要条件是：对任何 a,b 和 c，

$$b^{-1}[a,c]b=[a,c],$$

即 G 是一个亚阿贝尔群.

换位子群 群 G 中所有元素偶的换位元的集合所生成的子群 G' 称为群 G 的换位子群. 换位子群是一个全特征子群，因而也是

特征子群. 事实上,在群G的任意自同态χ下,元素a和b的换位元被映成元素

$$(a^{-1}b^{-1}ab)\chi=(a\chi)^{-1}(b\chi)^{-1}(a\chi)(b\chi),$$

等式右端的元素也是一个换位元.

换位子群的意义和下面的定理有关.

一个群对其换位子群的商群是阿贝尔群;反之,如果这个群对某一正规子群的商群是阿贝尔群,则换位子群包含在这个正规子群内.

事实上,如果a和b是群G中两个元素,则

$$aG'\cdot bG'=abG'=ba[a,b]G'=baG'=bG'\cdot aG',$$

因为元素$[a, b]$包含在换位子群G'内. 另一方面,如果商群G/N是阿贝尔群,则G中任意一对元素的换位元包含在N内,因而$G'\subseteq N$.

根据§10中所建立的正规子群和商群之间的关系,由这个定理的第一部分可以看出: *群G中任何一个包含G的换位子群的子群是群G的正规子群.*

利用换位子群的定义和上面所证明的定理,还可以对亚阿贝尔群的定义给出两种新的说法:

群G是一个亚阿贝尔群的充分必要条件是它的换位子群包含在中心内.

群G是一个亚阿贝尔群的充分必要条件是它对中心的商群是阿贝尔群.

群G的换位子群等于单位群E,当且仅当G是阿贝尔群,也就是说,当且仅当G和自己的中心相重合。然而换位子群和中心的这一关系却不能倒转过来:即由中心和单位子群相重合不能推出换位子群和整个群相重合,虽然初看起来这好像是很自然的. 例如:在:如$n\geqslant 3$时对称群S_n是无中心群,可是它的换位子群却是

交错群 A_n. 对 $n=3$ 和 4 的情形可以用直接验证的方法来证明，对 $n\geq5$ 的情形，可以用下面的方法来证明：商群 S_n/A_n 是一个 2 阶循环群，因而是一个阿贝尔群. 由此根据以上所证可知，群 S_n 的换位子群包含在 A_n 内. 但因为 S_n 是非交换群，而 A_n 是单纯群，故 S_n 的换位子群和 A_n 相重合. 与此完全相同，由换位子群和整个群相重合不能推出中心和单位子群相重合. 这方面的一个很好的例子就是行列式等于 $+1$ 的复系数 $n>1$ 阶矩阵的乘法群，但我们不作详细的讨论.

由换位子群的定义可以直接推出下面的事实：*子群的换位子群永远包含在整个群的换位子群内.*

设 G' 是群 G 的换位子群. 群 G' 的换位子群 G'' 称为群 G 的*第二换位子群*. 这样类推下去，我们可得出群 G 的一个*递降子群序列*，这个子群列称为群 G 的*换位子群链*. 如果对非极限序数 α，我们把群 G 的第 α 个换位子群定义作群 $G^{(\alpha-1)}$ 的换位子群，对极限序数 α 则把它定义作所有 $G^{(\beta)}$ $(\beta<\alpha)$ 的交，则群的换位子群链一般是可以超穷地继续下去的. 存在一个序数 τ，其势不大于群 G 本身的势且使

$$G^{(\tau)}=G^{(\tau+1)},$$

也就是说，使换位子群链稳定下来. Мальцев[7] 证明，任意给出一个序数 τ，可以找到一个群 G，使其换位子群链刚好在序数 τ 上稳定下来.

群 G 的依次各个换位子群都是它的全特征子群.

为了证明这一命题，只须利用这样一个事实，即一个群是另一群的全特征子群这一性质是可传的，且在求交的运算下不变.

设 A 和 B 是群 G 中两个任意的子集. 由所有 $[a, b]$，$a\in A$，$b\in B$，这种形式的换位元所生成的子群，我们称之为这两个子集

的相互换位子群$[A,B]$,这样一来,我们就有

$$G'=[G,G].$$

利用这一概念，我们还可以造出另外一个由群G中的全特征子群所构成的递降子群序列，即群G的下中心链．这就是子群列

$$G=G_0\supseteq G_1\supseteq G_2\supseteq\cdots\supseteq G_\alpha\supseteq\cdots,$$

其中

$$G_\alpha=[G_{\alpha-1},G],$$

而在α是极限序数时，则G_α是所有$G_\beta(\beta<\alpha)$的交．这样一来，$G_1=[G,G]$,也就是说,G_1和群G的换位子群G'相重合;$G_2=[G_1,G]$,也就是说,G_2是换位子群G'和群G的相互换位子群，依此类推．这个子群链也在某一序数σ上稳定下来；并且对任意一个序数σ,可找到一个群G,使其下中心链刚好在这个序数上稳定下来(Мальцев[7]).

群G的下中心链中所有的项都是G的全特征子群.

设对所有$G_\beta(\beta<\alpha)$这一命题都已证明．如果α是极限序数,则只要利用全特征子群的交仍旧是全特征子群这一事实，就可以证明G_α是全特征子群；如果序数$\alpha-1$存在,则子群G_α由$[a,g]$这种形式的换位元生成,这里$a\in G_{\alpha-1}$, $g\in G$．如果φ是群G的一个任意的自同态,则

$$[a,g]\varphi=[a\varphi,g\varphi];$$

但$a\varphi\subset G_{\alpha-1}$, $g\varphi$是群G中的元素,故

$$[a\varphi,g\varphi]\in G_\alpha,$$

也就是说,$G_\alpha\varphi\subseteq G_\alpha$.

利用下中心链的概念，还可以给出亚阿贝尔群的定义的另一表述方式:

群G是一个亚阿贝尔群的充分必要条件是它的下中心链中的第二项是单位子群.

事实上，等式$[G', G]=E$和换位子群包含在中心内这一断语等效.

在P. Hall[2] 和 Головин[3] 的论文中，读者可以见到子群偶的相互换位子群的各种性质，以及这一概念的某些推广. [参看补充 3.3.]

§15. 带运算子的群

群G中正规子群、特征子群和全特征子群，对群G的内自同构群、所有自同构的群和所有自同态的集合而言，起着彼此类似的作用. 这一事实的最自然的推广就是取出群G的一组自同态V，而研究所有V-特征子群，即在V的所有自同态下映入其自身的子群. 我们有时要采用这一办法；然而在各方面的应用上——在环论中，在线性代数中等等——有更大意义的是这一办法的更进一步的推广，即研究带运算子的群.

假设已知一个群G和一组符号Σ: σ, τ, $\cdots$. 如果对Σ中每个符号σ，有群G中一个自同态与之对应，也就是说，对群G中任何元素a，有同一群中的元素$a\sigma$与之对应，并且

$$(ab)\sigma=a\sigma\cdot b\sigma$$

则群G称为带运算子区Σ的群，而Σ中的符号则称为这个群的运算子.

在这里，同一自同态可能和Σ中不同的运算子相对应，也就是说，在$\sigma\neq\tau$时，可能对G中所有的a有$a\sigma=a\tau$. 和研究仅仅取出一组自同态的群比较起来，带运算子的群的研究之所以是一个推广也就在于此.

带同一运算子区的群G和$\bar{G}$称为带运算子同构，如果他们彼此同构，并且这个同构对应可以这样地建立起来，使得对群G和$\bar{G}$中任意两个相互对应的元素a和$\bar{a}$，和Σ中任何σ，元素$a\sigma$和$\bar{a}\sigma$

相互对应.

在研究带运算子的群时，只有带运算子同构的群才被看作彼此恒等. 这样，一个在普通意义下的群可能给出任意多个互不相同的带运算子的群. 初看起来，群的概念的这一分化，好像和我们将群运算的概念特别提出来作为实际研究对象所达到的普遍性相违背. 然而，我们将会看到，在许多重要的群论定理中要断定某些群(或子群)的同构时，在带运算子群的情况下，这一同构同时也是带运算子同构. 不难理解，如果将这些定理对带运算子的群表述出来并加以证明，我们就可以达到更大的普遍性，因要想对不带运算子的群得出相应的定理，只要设运算子的集合是一个空集合就行.

假设已经给定一个带运算子区Σ的群G，而V_Σ是和Σ中的运算子相对应的群G的自同态的集合. 群G的V_Σ-特征子群称为这个群对运算子区Σ的*容许子群*，换句话说，如果对Σ中所有的σ，它在包含元素a的同时，也包含元素$a\sigma$，也就是说，如果

$$H\sigma\subseteq H,$$

则群G的子群H就是一个容许子群. 因此，Σ中任何一个运算子在每一个容许子群中引出一个自同态. 由于这一点，群G中的容许子群可看作是带同一运算子区Σ的带运算子群. 全特征子群在任何一组运算子下都是容许子群，并且只有他们才有这一性质. 举例来说：如在上一节中所证，群的中心就不永远是容许子群.

例 1：如果取群的内自同构作为它的运算子，正规子群就是容许子群. 若取群的所有自同构作为运算子时，特征子群就是容许子群，而如果运算子区是它的所有自同态的集合时，只有全特征子群才是容许子群.

例 2: 假设已经给出一个环 R, 这个环可能是非交换的. 不难验证, 如果将环 R 中所有元素都在右侧乘上 R 中某一个固定元素 a, 则 R 的加法群就受到一个自同态映射. 因此, 环 R 本身就是它自己的加法群的一个运算子区, 此时右理想就是容许子群. 将环中所有元素从左侧乘上 R 中元素 a 时, 同样也能引出这个环的加法群的一个自同态. 因此, 环 R 的元素还组成它的加法群的另外一个运算子区;对于这个运算子区左理想是容许子群. 将这两个运算子的集合联合在一起时——环中任何一个元素显然要作为两个运算子取出两次——得出一个新的运算子区,对于它,容许子群是双侧理想.

例 3: 域 P 上任何矢量空间 V 是一个以域 P 作运算子区的带运算子阿贝尔群. 事实上, 在矢量空间的定义中就包括条件

$$(a+b)\alpha=a\alpha+b\alpha,$$

其中 $a,b\in V\alpha\in P$. 容许子群是线性子空间.

例 4: 任何一个阿贝尔群都可看作一个以整数环 C 作运算子区的带运算子群. 和整数 n 相应的自同态就是将元素 a 变为 a^n (如果在加法表示下, 则将元素 a 变成元素 na) 的映射. 事实上, 对于阿贝尔群,等式

$$(ab)^n=a^nb^n$$

成立. 在这一组运算子下任何子群都是容许子群.

由于运算子的引入, 从所考察的群的全体子群中就分化出它的容许子群来, 而从这个群的全体同构中则分化出带运算子同构来. 如果我们所考察的是带运算子区 Σ 的群 G, 且和 Σ 中的运算子相应的群 G 的自同态的集合是 V_Σ,则群 G 可以很自然地被看作带运算子区 V_Σ 的群, 并且由容许子群的定义可以看出, 对 Σ

和V_Σ的容许子群是群G中同样的一些子群. 这一注记使我们在必要时可以假定运算子的集合就是群的所有自同态集合的一个子集合. 而且，只有用上述对运算子区的一般定义，我们才能把任一环看作是它的加法群的运算子区(例 2). 事实上，环可能具有异于零的元素，它乘上任何元素之积都等于零.

前面就不带运算子的群所引入和证明的许多概念和某些定理可以推广到带运算子群的情形. 在这里，我们只举出那些在以后的论述中将要用到的概念和结果，而证明的细节则留给读者自行作出.

假设已经给出一个带运算子区Σ的群G. 对这个群的容许子群可以作以下断言:

任意一组容许子群的交是一个容许子群，包含群G一个已知集合M的所有容许子群之交称为由集合M生成的容许子群. 如果集合M由一个元素a组成，我们就得出元素a的容许循环子群，一般来说，这个子群不等于循环子群$\{a\}$. 由任何一组容许子群所生成的子群以及一个递增容许子群列的并集同样也是容许子群.

如果由集合M所生成的容许子群和群G本身重合，则M是群G对运算子区Σ的生成系. 应该注意的是，一个群对一个已知运算子区可能是具有限生成系的，尽管当作一个普通的群来看时，它可能不是一个具有限生成系的群. 例如，作为一个带运算子的群，域P上的n维矢量空间具有一个由n个元素组成的生成系——矢量空间的任何一组基都可作为生成系——但在P是一个非可数域时，群V也是非可数的，因而，作为一个不带运算子的群，它不可能具有一个有限生成系.

如果已经给出带同一运算子区的群

$$G_1, G_2, \cdots, G_n, \cdots,$$

且对每一个整数 n,群 G_n 在群 G_{n+1} 内已经建立了一个带运算子同构对应．则这些群的*极限群* $\bar{G}$(参看 §7)同样也是一个以 Σ 为运算子区的带运算子群,而群 $G_n(n=1, 2, \cdots)$ 则和群 $\bar{G}$ 中某些容许子群带运算子同构．

如果一个带运算子群的正规子群是它的一个容许子群,这个正规子群就称为*容许正规子群*．任意一组容许正规子群的交，和由这一组容许正规子群生成的子群都是容许正规子群．除自己本身和单位群之外,不再包含其它容许正规子群的群称为*单纯群*(对于一个已知的运算子区)．当然,如果把这个群当作不带运算子的群来考察时,它可能不是单纯的．

假定已经给定两个带同一运算子区 Σ 的群 G 和 G'，和带运算子同构相类似,群 G 到 G' 上的一个同态映射叫做一个*带运算子同态*，如果对 G 中任何元素 a 和它在 G' 中的像 a' 以及 Σ 中任何一个运算子 σ，元素 $a\sigma$ 在这个同态映射下的像是 $a'\sigma$．在这个同态下映成群 G' 中单位元 $1'$ 的群 G 中的正规子群是一个容许正规子群,因为由 $1'\sigma=1'$ 对 Σ 中所有 σ 都成立这一事实可以推出：这个正规子群在包含任意一个元素 a 的同时也包含所有元素 $a\sigma$．

反过来，假设带运算子区 Σ 的群 G 同态地映在一个群 G' 上,并且在这一同态下群 G 中映在群 G' 的单位元上的正规子群是一个容许子群。在这时 Σ 中的运算子可按下述方式转移到 G' 上：如果已经给定 G' 中一个元素 a' 和 Σ 中一个运算子 σ，我们可在 G 中取出元素 a' 的原像之一 a，并把元素 $a\sigma$ 的像记作 $a'\sigma$．不难看出，由于正规子群 H 是一个容许子群，所以元素 $a'\sigma$ 与元素 a 的选择无关．作为特例，我们可以得到这样一个结论，*即带运算子的群对其容许正规子群的任何商群，是具同一运算子区的带运算子群，并且，群在这个商群上的自然同态映射是一个带运算子同态*．

现在读者可以不困难地证明：若群 G 带运算子同态映成 G'，则 G' 和群 G 对某一容许正规子群的商群带运算子同构，即是说，可证明带运算子群的同态定理.

如果 H 是群 G 的一个容许正规子群，那末在群 G 中包含 H 的子群和商群 G/H 的子群之间的对应关系下，容许子群和容许子群相对应. 这一断言的证明可由上述将运算子转移于商群上的方法直接得出.

对带运算子群，同构定理同样也能保持：

如果 A 和 B 是带运算子群 G 的两个容许子群，且 A 是子群 $\{A, B\}$ 的正规子群，则交 $A\cap B$ 是 B 的正规子群，商群 $\{A, B\}/A$ 和 $B/(A\cap B)$ 带运算子同构.

这个定理的证明和在不带运算子群的情况下的证明一样. 带运算子同构可以当作带运算子群的同态定理的一个推论得出.

Zassenhaus 引理也可以推广到带运算子群上. 在它的陈述中还是要谈到容许子群和带运算子同构.

带运算子区 Σ 的群 G 到其自身上或到其自身内的任何一个带运算子同态，称为群 G 的一个带运算子自同态. 换句话说，如果对 G 中任何元素 a 和 Σ 中任何运算子 σ，等式

$$(a\sigma)\chi = (a\chi)\sigma, \tag{1}$$

成立，则自同态 χ 是一个带运算子自同态.

带运算子自同态的特例是带运算子自同构，也就是说，群 G 到其自身上的带运算子同构.

由带运算子自同态的定义可直接推出下面的定理，在这个定理中，“可换”二字应当理解作自同态乘法的可换性：

群 G 的自同态 χ 当且仅当它和所有与运算子区 Σ 中的运算子相应的自同态可换时，也就是说，当且仅当它和集合 V_Σ 中所有自同态可换时，才是对于 Σ 的一个带运算子同态.

要证明这个定理，只要在等式(1)中将运算子换成与之相应的自同态．作为一个例子，我们可以指出，域P上的矢量空间V的线性变换乃是带运算子自同态，因为线性交换的定义中刚好就有条件

$$(a+b)\varphi=a\varphi+b\varphi,\ (a\alpha)\varphi=(a\varphi)\alpha,$$

其中$a,b\in V$，$\alpha\in P$，φ是线性变换．

从这一定理不难推出带运算子自同态和自同构的一切性质．例如：两个带运算子自同态的积还是一个带运算子自同态．零化自同态永远是一个带运算子自同态．其次还要注意一点，单位(恒等)自同构和所有自同态可换，因此一定是一个带运算子自同构，带运算子自同构的逆自同构是一个带运算子自同构．关于带运算子自同态和自同构的乘积作了上述按语后，我们就可以谈论一个带运算子群的带运算子自同构的群．它是所有自同构群的一个子群．

最后要指出，带运算子群G的容许子群在带运算子自同态下的像同样也是一个容许子群，如果H是一个容许子群，也就是说，如果对所有的运算子σ

$$H\sigma\subseteq H,$$

则对带运算子自同态χ有

$$(H\chi)\sigma=(H\sigma)\chi\subseteq H\chi.$$

由此可知，$H\chi$是一个容许子群，而且，这个事实也可以由同态定理得出．

就其特例而言，群G本身在一个带运算子自同态下的像是它的一个容许子群．［参看§补充4.］

第五章　子群列·直积·定义关系

§16. 正规群列与合成群列

在群论和它的应用里，已知群的一个包含在另一个内的且又满足某种附加条件的子群系占着很重要的地位. 在这一节里，我们要研究这种有序子群系或子群"列"的一些性质. 这里所得到的结果在以后将有许多应用.

群 G 的始于 G 本身而终于单位子群 E 的一个包含在另一个内的子群的有限系

$$G=G_0\supset G_1\supset G_2\supset\cdots\supset G_k=E \quad (1)$$

叫做这个群的一个**正规群列**，假如每一个子群 G_i 都是 G_{i-1} 的一个正规真子群，$i=1, 2,\cdots, k$. 特别，子群 G_1 是群 G 的正规子群，G_2 是子群 G_1 的正规子群，尽管它不一定是 G 本身的正规子群等等.

显然，任何一个群都具有正规群列，——例如，只要取群列 $G\supset E$ 就可以了. 如果 H 是 G 的一个异于 G 也异于 E 的正规子群，那末群列

$$G\supset H\supset E$$

也是正规的. 换句话说，在任何一个群里，可以通过这个群的一个给定的正规子群而求得一个正规群列.

商群

$$\frac{G}{G_1}, \frac{G_1}{G_2}, \cdots, \frac{G_{k-1}}{E}$$

叫做正规群列(1)的**因子**. 这些因子的个数，即群列(1)中的数 k，叫做群列(1)的**长度**.

正规群列

$$G\supset F_1\supset F_2\supset\cdots\supset F_l=E \tag{2}$$

叫做正规群列(1)的加密，假如(1)中每一子群G_i都和子群F_j中之一重合，也就是说，假如(1)中所有子群也都在群列(2)中出现．特别，任意一个正规群列都是它本身的加密．在正规群列(1)和它的加密(2)的长度之间显然有不等式$k\leqslant l$.

一个群的两个正规群列说是同构的，假如它们的长度相同并且它们的因子可以这样地一一对应起来，使得相对应的因子是同构的群．在这个定义里，并没有假定所指出的对应要保持因子的相互位置．比如说，在六阶循环群$G=\{a\}, a^6=1$中，正规群列$G\supset\{a^2\}\supset E$与$G\supset\{a^3\}\supset E$同构，因为它们的因子是一个二阶循环群和一个三阶循环群，虽然在这两个群列中因子的位置是不一样的.

对于带运算子的群来说，上面所给出的一切定义都保持．当然，在正规群列的定义里必须提到容许子群和容许正规子群，而在群列同构的定义里要提到因子的带运算子同构．本节以下的一切内容都是在这样的假定之下陈述的，即*所考虑的群带有某一个(可能是空的)运算子集合*.

下面的定理在正规群列的理论中扮演一个基本的角色[1]:

Schreier 定理 *一个群的任意两个正规群列都具有同构的加密.*

事实上，设在群G中给定了正规群列

$$G=H_0\supset H_1\supset H_2\supset\cdots\supset H_k=E, \tag{3}$$

$$G=F_0\supset F_1\supset F_2\supset\cdots\supset F_l=E. \tag{4}$$

1) Schreier O. [5]. 本书中的证明是由 Zassenhaus[1]给出的.

引入以下记号:

$$H_{ij}=H_i\cdot(H_{i-1}\cap F_j),$$
$$F_{ij}=F_j\cdot(F_{j-1}\cap H_i),$$

此处 H_{ij} 与 F_{ij} 都是子群，因为，比方说 H_i 是 H_{i-1} 的正规子群而 $H_{i-1}\cap F_j$ 是 H_{i-1} 的子群. 于是对于 $i=1, 2, \cdots, k, j=1,2,\cdots,l$ 来说,包含关系

$$H_{i-1}=H_{i0}\supseteq H_{i,j-1}\supseteq H_{ij}\supseteq H_{il}=H_i,$$
$$F_{j-1}=F_{0j}\supseteq F_{i-1,j}\supseteq F_{ij}\supseteq F_{kj}=F_j$$

成立. 根据 Zassenhaus 引理(§ 10 与 § 15)，子群 H_{ij} 是 $H_{i,j-1}$ 的正规子群,子群 F_{ij} 是 $F_{i-1,j}$ 的正规子群,而对应的商群同构:

$$\frac{H_{i,j-1}}{H_{ij}}\simeq\frac{F_{i-1,j}}{F_{ij}}. \tag{5}$$

如果我们在群列(3)的两个子群 H_{i-1} 与 $H_i(i=1,2,\cdots,k)$之间嵌入一切 $H_{ij}(j=1,2,\cdots,l-1)$,那末就得到群(3)的一个加密,一般来说,这是一个*有重项的*正规群列,因为子群 $H_{i,j-1}$ 与 H_{ij}可能是相等的. 相应地，利用子群 F_{ij} 也可做成群列(4)的一个加密. 由(5),这样的两个加密是同构的. 为了结束证明，只要再从这两个加密中去掉重复的项就是了. 但是如果 $H_{i,j-1}=H_{ij}$,即若 $\frac{H_{i,j-1}}{H_{ij}}=E$,那末根据(5),$F_{i-1,j}=F_{ij}$,因此,不破坏所得到的群列(3)与(4)的加密的同构性，我们可以同时从它们中间去掉所有的重复项. Schreier 定理证毕.

若一个正规群列不再有异于它本身的(无重项的)加密，这群列就叫做一个*合成群列*. 换一句话说,如果群列

$$G=G_0\supset G_1\supset G_2\supset\cdots\supset G_k=E$$

中任意一个子群 G_i, $i=1,2,\cdots,k$,都是子群 G_{i-1} 的*极大正规真子群*，那末这个群列是 G 的一个合成群列. 合成群列的每一个因子

显然都是单纯群. 反过来,任何一个正规群列,如果它的所有因子都是单纯群,就不可能再加密, 因而是一个合成群列. 因此,任何一个与某一合成群列同构的正规群列,本身也是一个合成群列.

从 Schreier 定理直接得出以下定理:

Jordan-Hölder 定理 *如果群 G 有合成群列,那末这个群的任意两个合成群列是同构的.*

事实上, 所给这一对合成群列的同构加密与这两个群列重合.

如果群 G 有合成群列, 那末这个群的任意正规群列都被包含在某一合成群列中,因而它的长度不超过群 G 的合成群列的长度.

为了证明这一点, 只要把 Schreier 定理应用到所给的正规群列和这个群的一个合成群列上就够了.

为了简单起见, 我们约定把一个具有合成群列的群的合成群列的共同长度,叫做这个群的*合成长度*,而注意一个合成群列的因子就叫做这个群的*合成因子*.

合成群列远不是任意群都有的. 例如,在无限循环群中,任何一个正规群列就已经有异于它自己的加密了. 事实上, 在这个群列的倒数第二个位置上的子群一定是一个无限循环群, 因而在它和单位子群之间可以嵌入一串补充的子群. 一般来讲, 一个具有合成群列的、不带运算子的阿贝尔群一定是有限的,因为这个群的合成因子只能是素数阶的循环群. 一般地, 任意一个有限群显然都有合成群列. 其次, 对于任意一个单纯群 G 来说——无限单纯群的存在性已在 §9 中证明——,唯一的合成群列就是 $G \supset E$. 我们现在证明, 群有合成群列的一个简单的充分必要条件. 首先引入一个新的定义.

群 G 的子群 H 叫做一个*可届子群*, 假如它被包含在 G 的某一正规群列内. 换句话说,群 G 的所有正规子群,这些正规子群的所

有正规子群等等就是群G的可届子群. 显然，可届子群的正规子群也是可届子群. [参看补充 2.6.]

群G的递降子群列

$$G=H_0\supset H_1\supset H_2\supset\cdots\supset H_n\supset\cdots \tag{6}$$

叫做群G的一个正规降链，假如每一个子群H_n, $n=1,2,\cdots$, 都是H_{n-1}的正规真子群. 正规降链或者是可数的，按自然数列序型整列的，或者是有限的. 在后一情形就说，这个链是断的. 任何一个正规群列都是断正规链的例子. 无限循环群$G=\{a\}$的如下子群列

$$G\supset\{a^2\}\supset\{a^4\}\supset\cdots\supset\{a^{2n}\}\supset\cdots$$

可以作为一个无限正规降链的例子.

群G的递升子群列

$$E\subset F_1\subset F_2\subset\cdots\subset F_n\subset\cdots \tag{7}$$

叫做群G的一个正规升链，假如任何一个子群F_n, $n=1,2,\cdots$, 都是F_{n+1}的正规真子群，并且所有子群F_n都是群G的可届子群[1). 正规升链可能是无限的，——例如，在有理数加法群里可以找到这样的链，——也可能是有限的，也就是断的.

群G当且仅当它的一切正规降链和一切正规升链都是断的时候，才有合成群列.

事实上，设群G有合成群列，并且设k是它的合成群列的长度. 如果群G有一个无限正规降链(6)，那末当$n\geqslant k$时，由群列(6)的前面几项及单位子群所构成的正规群列

$$G\supset H_1\supset H_2\supset\cdots\supset H_n\supset E$$

的长度超过k. 然而这是与Schreier定理相违的. 其次，假定群G有一个无限正规升链(7). 那末取$n\geqslant k$并且做群G的一个含有子群F_n的正规群列:

---

1) 最后的要求在正规降链的情形是自动满足的.

$$G \supset G_1 \supset \cdots \supset G_{s-1} \supset F_n \supset \cdots \supset E, s \geqslant 1.$$

这样的群列是存在的，因为根据条件，F_n 是可届子群. 于是群列

$$G \supset G_1 \supset \cdots \supset G_{s-1} \supset F_n \supset F_{n-1} \supset \cdots \supset F_2 \supset F_1 \supset E$$

是正规的，并且它的长度大于 k，这仍旧与 Schreier 定理矛盾.

现在假定在群 G 里，一切正规降链和一切正规升链都是断的. 由于升链是断的，我们推出，在群 G 的任何一个可届子群 H 里，总可以找到这个子群的一个极大正规真子群. 事实上，如果子群 H 的任何一个正规真子群都被包含在 H 的某一较大的正规真子群内，那末我们将得到子群 H 的一个无限正规升链，它将是 G 的一个正规升链.

现在所求的合成群列可以如下地构成: 在群 G 里，取出一个极大的正规真子群 H_1. 设已经选出子群

$$H_0 = G, H_1, H_2, \cdots, H_n,$$

其中每一个都是它前面一个的极大正规真子群; 子群 H_n 显然是 G 中一个可届子群. 于是，若 $H_n \neq E$，那末我们就取子群 H_n 的一个极大正规真子群作为 H_{n+1}. 由于正规降链是断的，经过有限多步以后，我们就达到子群 E，这就是说，我们得到群 G 的一个合成群列. 定理证毕.

如果一个群具有合成群列，那末关于它的子群，我们能够说些什么? 可数交错群的例子(参看 § 4)告诉我们，一个具有合成群列的群可能包含一个没有合成群列的子群. 事实上，所说的群是单纯的(参看 § 9)，这就是说，它具有合成群列，但是它的由置换

$$b_n = (4n-3, 4n-2)(4n-1, 4n), n = 1, 2, \cdots,$$

所生成的子群是无限的并且是一个阿贝尔群——后一论断是由于一切元素 b_n 的可换性——，因此它不可能具有合成群列.

但是一个具有合成群列的群 G 的任何一个可届子群 H 也具有合成群列. 事实上，子群 H 包含在群 G 的某一正规群列内，根据所

作的假定，这个正规群列可以加密为合成群列. 这个合成群列在子群H与单位子群之间的一段就是H的一个合成群列. 由此还推出，如果H是群G的一个可届真子群，那末群H的合成长度小于群G的合成长度，而群H的合成因子是由G的合成因子系的一部分所组成的. 另一方面，如果H是群G的正规子群，那末包含H的合成群列在G与H之间的那一段就导出商群$\frac{G}{H}$的一个合成群列. 由此得出，具有合成群列的群G的任何一个商群$\frac{G}{H}$也具有合成群列；它的合成长度等于群G的合成长度与群H的合成长度之差，而它的合成因子连同群H的合成因子一起构成群G的一个合成因子系.

就具有合成群列的群来说，我们可以从下列定理得出关于其任意子群的一些结论. 以下的定理是关于任意群来说的:

设在群G中给定了一个正规群列

$$G=G_0\supset G_1\supset G_2\supset\cdots\supset G_k=E, \tag{8}$$

那末群G的任何一个子群F都具有正规群列，它的因子与群列(8)中某些不同的因子的子群同构.

事实上，设$F_i=F\cap G_i$, $i=0,1,2,\cdots,k$, 那末在$A=F$, $A'=E$, $B=G_{i-1}$, $B'=G_i$的情形下应用 Zassenhaus 引理，我们得到，F_i是F_{i-1}的正规子群并且

$$\frac{F_{i-1}}{F_i}\simeq\frac{G_iF_{i-1}}{G_i}.$$

但是$G_{i-1}\supseteq G_iF_{i-1}\supseteq G_i$，这就是说，商群$\frac{F_{i-1}}{F_i}$与商群$\frac{G_{i-1}}{G_i}$的一个子群同构. 因此，群列

$$F=F_0\supseteq F_1\supseteq F_2\supseteq\cdots\supseteq F_k=E$$

经过去掉可能的重复项以后，就是我们所求的F的一个正规群列.

上面得出的 Schreier 定理和 Jordan-Hölder 定理以及它们的推论是关于带任意运算子区的群的. 如果再把所有内自同构加到运算子区上去,那末容许子群只是正规子群. 在这一情形,合成群列的概念就转化为主群列的概念: 群 G 的子群序列

$$G=H_0\supset H_1\supset H_2\supset\cdots\supset H_k=E$$

叫做群 G 的一个*主群列*, 假如任何一个 $H_i(i=1, 2, \cdots, k)$ 作为包含在 H_{i-1} 内的真子群都是群 G 的一个极大正规子群. 上面所证明的关于合成群列的存在条件在这情形下转化为以下的定理:

群 G 当且仅当它的所有正规子群的降链和升链都是断链时,才有主群列.

这样的链在以下将分别叫做群 G 的*不变降链*和*不变升链*.

Jordan-Hölder 定理在所考虑的情形下化为以下定理.

若群 G 具有主群列,那末这个群的任意两个主群列都同构.

以前所建立的关于一个群的合成群列与它的可届子群之间的关联不能转到主群列的情形. 事实上,如果群 G 具有主群列,我们取经过一个给定子群 H 的主群列, 那末这个群列在 H 与 E 之间的一段可能已经不再是 H 的主群列了,因为一般来说,在 H 中存在这样的正规子群,它不是 G 的正规子群.

如果运算子区包含群 G 的所有自同构(或所有的自同态), 那末合成群列的概念就转化为*特征子群列*(相应的, *全特征子群列*)的概念,就是群 G 的这样的子群序列,其中每一个子群作为包含在它前面一个内的真子群,都是群 G 的一个极大特征(全特征)子群. 由 Jordan-Hölder 定理,在这一情形,我们得出以下定理:

若群 G 具有特征(全特征)子群列, 那末这个群的任意两个特征(全特征)子群列都同构.

这一节的结果的进一步的发展, 读者将在 §56 中找到. [参看补充 2.5.]

§17. 直　积

直积或(在加法群的情形)直和的概念是一般群论的最重要概念之一,特别地,它是群的某些分支,例如阿贝尔群的理论的基础. 在这一节里,我们将给出这个概念的定义并且指出它的一些最简单的性质,至于它的更深邃的理论将要在第十一章里单独阐述.

群G叫做它的子群$H_1, H_2, \cdots, H_n$的直积,假如以下三点要求被满足:

1) 子群$H_1, H_2, \cdots, H_n$都是群G的正规子群.

2) 群G是由子群$H_1, H_2, \cdots, H_n$所生成的.

3) 任意一个子群$H_i(i=1,2,\cdots,n)$与一切子群$H_j(j\neq i)$所生成子群的交等于E.

这个定义可以用下面和它等价的形式给出: 群G是它的子群$H_1, H_2, \cdots, H_n$的直积,假如

1') 任意两个子群H_i与$H_j(i\neq j)$的元素彼此可换.

2') 群G的任意元素g可唯一地写成乘积

$$g=h_1h_2\cdots h_n$$

的形式,此处$h_i\in H_i$, $i=1,2,\cdots,n$.

我们证明,由第一个定义可推出第二个定义. 为了证明条件1'成立,我们取元素$a\in H_i$, $b\in H_j$, $i\neq j$. 那末根据条件1,我们有$aba^{-1}\in H_j, ba^{-1}b^{-1}\in H_i$,这就是说,换位元$aba^{-1}b^{-1}$包含在交$H_i\cap H_j$之中,这个交根据条件3,应该等于$E$. 为了证明条件2'成立,我们注意,$G$的任意元素$g$写成乘积$g=h_1h_2\cdots h_n$的可能性由条件2及已经证明了的条件1'可以推出. 这种写法的唯一性可这样推出,假定

$$g=h_1h_2\cdots h_n=h'_1h'_2\cdots h'_n,$$

并且假定,比方说,$h_1\neq h'_1$,那末再一次利用1',我们得到等式

$$h_1'^{-1}h_1=(h_2'\cdots h_n')(h_2\cdots h_n)^{-1}$$
$$=(h_2'h_2^{-1})\cdots(h_n'h_n^{-1}),$$

这与条件 3 矛盾.

反过来,由直积的第二个定义可以推出第一个定义. 事实上,条件 2 蕴含在条件 2′ 中. 为了证明条件 3,我们假定,比方说,子群 H_1 与子群 $H_2, \cdots, H_n$ 所生成的子群的交含有一个不等于单位元的元素 c. 这个元素包含在 H_1 中,并且根据条件 1′,它同时又可以写成乘积 $h_2\cdots h_n$ 的形式,但是这与条件 2′ 矛盾. 为了证明条件 1,我们由 H_i 中取出元素 $\bar{h}_i$ 并且由 G 中取出任意元素 g. 由 2′, $g=h_1h_2\cdots h_i\cdots h_n$, 于是由 1′,

$$g^{-1}\bar{h}_ig=h_i^{-1}\bar{h}_ih_i\in H_i.$$

检验一个群 G 是不是它的子群 $H_1, H_2, \cdots H_n$ 的直积时,由于可用下面较弱的条件来代替第一个定义中的条件 3,做起来就方便得多.

3_0) 子群 $H_i(i=1,2,\cdots,n)$ 与子群 $H_1,\cdots,H_{i-1}$ 所生成的子群的交等于 E.

为了证明这一点,我们只需指出,由条件 1、2 及 3_0 就已经能够推出条件 1′ 及 2′. 因为由 3_0,我们立刻得到,若 $i\neq j$,则 $H_i\cap H_j=E$,于是条件 1′ 就被证明了,而只要再证明条件 2′ 中所述的唯一性. 如果对于元素 g 我们找到了两种不同的写法,

$$g=h_1h_2\cdots h_n=h_1'h_2'\cdots h_n'$$

并且设 $h_k\neq h_k'$,但 $h_{k+1}=h_{k+1}',\cdots,h_n=h_n'$, $k\leqslant n$,那末我们得到等式

$$h_k'^{-1}h_k=(h_1'h_1^{-1})(h_2'h_2^{-1})\cdots(h_{k-1}'h_{k-1}^{-1}),$$

这与条件 3_0 矛盾.

如果群 G 被分解为子群 $H_1, H_2, \cdots, H_n$ 的直积,那末这些子群就叫做出现在这个分解式中的直因子,而这个分解式就写为

$$G=H_1\times H_2\times\cdots\times H_n$$

的形式.

直积的定义是在分解为有限个直因子的情形下给出的. 但是这个概念对于无限多个直因子的情形也适用，并且按以下定义给出：群G叫做它的一组子群H_α(α遍历一个给定的足标集)的直积，并且记作

$$G=\prod_\alpha H_\alpha,$$

假如G是由这些子群所生成的，并且G中任何一个由有限多个子群H_α所生成的子群都是它们的直积. 由这个定义我们立刻可以推出不同的子群H_α中元素的可换性和把G中任意元素唯一地(不计因子的次序)写成由子群H_α中取出的某些有限多个元素的乘积的可能性. 其次，容易看出，每一个子群H_α都是G的正规子群：设g是G的任意元素，那末$g=h_{\alpha_1}h_{\alpha_2}\cdots h_{\alpha_k}$，但因为根据假设，$H_\alpha$，$H_{\alpha_1}$，$H_{\alpha_2}$，…，$H_{\alpha_k}$这些子群在群$G$中构成一个直积，所以$g^{-1}H_\alpha g=H_\alpha$. 用同样的方法可以证明，任意子群$H_\alpha$与一切$H_{\alpha'}$($\alpha'\neq\alpha$)所生成的子群的交等于$E$.

利用这一解释，可以指出和上面定义等价的无限多个子群直积的某些新定义，而并不需要预先考虑有限个因子的情形. 例如，和上面对于有限多个因子的情形的定义之一相当，读者不难证明，群G当且仅当在这样的情形下才是它的子群H_α的直积：1) 任意两个不同的子群H_α的元素彼此可换；2) G中任何一个元素都可以唯一地(若不计因子的次序)写成由子群H_α中所取出的有限多个元素乘积的形式.

我们指出由定义推出来的关于直积的最简单的性质：

I. 若

$$G=\prod_\alpha H_\alpha, \tag{1}$$

而因子 H_α 本身又可以分解为直积，

$$H_\alpha=\prod_\beta H_{\alpha\beta}{}^{1)},$$

那末群 G 是一切子群 $H_{\alpha\beta}$ 的直积，这里 $H_{\alpha\beta}$ 取遍所有的 α 及 β.

群 G 的这一新的直分解叫做分解式(1)的接续.

II. 若(1)是群 G 的一个直分解，那末可以这样地得到它的一个新的直分解，用任意方式把子群 H_α 的集合分成一些互不相交的部分集合，并且把出现在这些部分集合的每一个里的子群 H_α 用它们的直积来代替.

III. 若在分解式(1)的每一个直因子 H_α 中选出一个子群 H'_α，$E\subseteq H'_\alpha\subseteq H_\alpha$，那末一切子群 H'_α 在群 G 中所生成的子群是这些子群的直积.

如果 $G=H_1\times H_2\times\cdots\times H_n$，那末 G 中任意元素 g 都可写成 $g=h_1h_2\cdots h_n$ 的形式，此处 $h_i\in H_i, i=1,2,\cdots, n$. 唯一确定的元素 h_i 叫做元素 g 在直因子 H_i 中的分支. 由此看出，元素 g 在 H_i 中的分支与所给的分解有关：如果给出群 G 的另一个也包含 H_i 作为一个直因子的直分解，那末 g 在 H_i 中的分支可能不再是 h 了. 对于具有无限多个直因子的直积来说，元素的分支的概念仍旧保持，但是应该记住，在这时每一元素在给定的直分解之下只有有限多个异于 1 的分支.

若 $G=\prod\limits_\alpha H_\alpha$，并且设 F 是群 G 的任意一个子群，那末子群 F 的一切元素在直因子 H_α 中的分支所成的集合 F_α 是一个子群. 这个子群叫做子群 F 在 H_α 中的分支。如果 F 是群 G 的正规子群，那末子群 F_α 是 H_α 的正规子群并且也是 G 的正规子群. 后一论断由下面的直积的一般性质导出：

1) 自然，H_α 中的某些个实际上可能是不可分解的.

IV. 若A是群G的一个直因子，那末子群A的任何一个正规子群A'也是G的正规子群.

事实上，在G中存在这样的子群B，使得$G=A\times B$. 若g是G的任意元素而$g=ab$，$a\in A$，$b\in B$，那末

$$g^{-1}A'g=a^{-1}A'a=A'.$$

因属于一个给定直分解的不同直因子的元素是可换的，我们可由此推出，直积的元素相乘时，就是它们对应的分支相乘. 因此，特别地，直积的两个元素的换位元的分支等于这两个元素分支的换位元. 由此推出

V. 直积的换位子群等于它的因子的换位子群的直积.

另一方面，由上述关于两个元素的换位元的分支的性质得出，直积中两个可换元素的分支也彼此可换，因此

VI. 直积的中心等于它的因子的中心的直积.

事实上，如果元素z属于群$G=\prod_{\alpha}A_\alpha$的中心，那末元素z在A_α中的分支z_α将与G中任意元素的分支，即与A_α中任意元素可换.

若F是直积的一个子群，那末F包含在它的分支的直积之中. 在一般情况下，它并不等于这个直积. 如果子群F的所有分支都包含在F中，亦即若F的所有分支与F和对应直因子的交重合，在这一情况下，可以推出F与它的分支的直积重合. 我们甚至可以证明以下性质.

VII. 若$G=A\times B$且子群F在A中的分支与交$F\cap A$重合，那末F在B中的分支与交$F\cap B$重合，而F是这两个交的直积.

事实上，若$f\in F$而$f=ab$，那末$b=a^{-1}f\in F$，因为根据条件$a\in F$.

由此推出

VII′. 若 $G=A\times B$ 而子群 F 包含直因子 A, 那末 $F=A\times(F\cap B)$.

最后我们指出性质

VIII. 若 $G=A\times B$, 那末直因子 B 与商群 $\frac{G}{A}$ 同构.

事实上, 设 Ag 是群 G 对子群 A 的一个陪集并且 $g=ab$, 那末 $b\in Ag$, 这就是说, 群 G 对 A 的任何一个陪集都含有 B 的一个元素并且, 很明显, 只含有一个 B 的元素.

到现在为止, 我们只谈论某一个群分解为它的子群的直积. 以下我们常常要谈到某些给定的群的直积. 例如, 假定已知群 A 和 B. 一切可能的元素对 (a,b) 的集合, 此处 a 是 A 中的元素, b 是 B 中的元素, 在如下定义的运算之下作成一个群:

$$(a,b)\cdot(a',b')=(aa',bb').$$

容易验证, 这个群是它的子群 A' 与 B' 的直积, 其中 A' 是由形式如 $(a,1)$ 的元素偶所构成的, 而 B' 是由形式如 $(1,b)$ 的元素偶所构成的[1]. 所指出的子群分别与已知群 A 和 B 同构, 因此我们所作成的群可以, 并且以后就叫做群 A 与 B 的直积. 这种构成法可以毫无困难地用到任意有限个已知群的情形. 这种构成法对无限多个群的情形可如下来作: 假设任意给定一组群 A_α, 那末这些群的直积的元素是由每一个 A_α 中取出一个元素 a_α 所组成的元素系, 并且所有这些元素, 除去有限个外, 都是相应子群的单位元. 这样的元素系的乘法定义一如有限多个直因子的情形.

我们所阐述的由一些已知群通过作直积而得到新的群的方法在以后将要有许多应用.

在所指出的无限多个群的直积的构成里, 显然可以去掉只有

1) 在元素偶 $(a,1)$ 中, 元素 1 显然是群 B 的单位元, 在元素偶 $(1,b)$ 中, 1 是群 A 的单位元.

有限多个分支异于单位元这一要求，而考虑由每一个已知群 A_α 里取出一个元素所构成的任意元素系. 这样得到的群叫做所给群的完全直积；在 Граев 的论文[1]中指出了这种群的一些有趣的性质. 然而应该注意的是，对于完全直积来说，就不可能像上面对普通直积那样来给出《内部的》定义. [参看补充 6.1.]

直积的这两种类型可以统一在以下的带分出子群的直积这一构造中：在每一个给定的群 A_α 里，假定分出某一个子群 B_α，$E\subseteq B_\alpha\subseteq A_\alpha$. 考虑从每一个群 A_α 中取出一个元素所组成的元素系，这些元素只有有限多个在对应的子群 B_α 外，而乘法，就像上面一样，是按分支相乘. 由 Виленкин[1] 所引入的这种构造在拓扑阿贝尔群中有着重要的应用.

一个群，如果不能分解为它的真子群的直积，就叫做不可分解的，或者确切一点说，叫做不能分解成直积的，因为以后我们还要遇到其他形式的乘积. 显然，一切单纯群都是不可分解的群. 有理数加法群，同样地，整数加法群，即无限循环群的不可分解性是这样得出的：对于任意两个有理数都存在异于零的公倍数，因而这个群的任意两个异于零的子群的交也异于零.

若给定一个 p^m 阶的循环群 $\{a\}$，这里 p 是一个素数，那末这个群的所有异于 E 的子群就是元素 $a, a^p, a^{p^2}, \cdots, a^{p^{m-1}}$ 的循环子群. 换句话说，如果给出这个群的任意两个子群，那末其中一个必定包含在另外一个之中. 由此推出，p^m 阶循环群，同样地，p^∞ 型群是不可分解的.

另一方面，任意一个阶为合数的循环群都可以分解为一些循环群的直积，它们的阶都是不同素数的幂.

事实上，令

$$n=p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$$

是循环群 $\{a\}$ 的阶，此处 $s\geqslant 2$，而 $p_1, p_2, \cdots, p_s$ 是互不相同的素数.

引入记法

$$q_i = p_1^{m_1} \cdots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \cdots p_s^{m_s}, \ i = 1, 2, \cdots, s.$$

元素 a^{q_i} 有阶 $p_i^{m_i}$. 循环子群$\{a^{q_i}\}$与所有循环子群$\{a^{q_j}\}(j \neq i)$的乘积的交是 E，因为所说乘积中所有元素的阶都与 p_i 互素. 因此，在群$\{a\}$中，子群$\{a^{q_i}\}(i=1, 2, \cdots, s)$的积是直积且确实与群$\{a\}$重合，因为直积的阶等于直因子的阶的乘积.

可分解群的另一些例子是可分解为实数加法群与虚数加法群的直和的复数加法群，以及可分解为正实数乘法群及由-1所生成的二阶循环群的直积的非零实数乘法群. 正有理数乘法群可以分解为可数个无限循环群的直积，这些循环群是由不同的素数所生成的. 还要指出，我们已经不止一次地遇到过的 4 阶非循环的阿贝尔群是两个 2 阶循环群的直积.

直积的概念也可用到带运算子的群上. 在这一情形下，显然只限于考虑这样的可分解为直积的群，它的一切直因子都是对于所考虑的运算子区的容许子群. 另一方面，如果给出了带同一运算子区 Σ 的一些群 A_α，那末这些群的直积 G 也可以看成是带同一运算子区的带运算子的群，不过要假定

$$g = a_{\alpha_1} a_{\alpha_2} \cdots a_{\alpha_k}, \ g \in G, \ a_{\alpha_i} \in A_{\alpha_i},$$

以使

$$g\omega = a_{\alpha_1}\omega \cdot a_{\alpha_2}\omega \cdots a_{\alpha_k}\omega,$$

此处 $\omega \in \Sigma$. 特别地，由这个等式推出，容许子群的分支也是容许子群.

以后我们就会知道(§ 26)，存在这样的可分解的群，它不可能分解为一些不可分解群的直积，于是就发生了一个群在什么条件下具有这样的分解的问题. 另一方面，一个群也可以有许多不同的这种分解. 这就引起关于一个群分解为不可分解因子的直积的唯一性问题. 再者，一个群的两个直分解叫做同构的，假如在这两

个分解的因子之间可以建立这样的一个相互单值对应，使得对应的因子是彼此同构的群．关于一个群的任意两个分解成不可分解因子的直分解在什么条件下是同构的问题，或者更一般地，关于任意两个直分解在什么条件下具有同构延拓的问题，曾是许多研究工作的对象．所有这些问题都将在第十一章里加以讨论，而对于各类阿贝尔群的同样的讨论将在第六章到第八章里进行．

§ 18. 自由群·定义关系

这一节的目的是要建立一些给出群的方法，使我们不必利用定义了群运算的集合的元素的个别性质．为了达到这一目的，首先必须构成一类特殊的群，叫做自由群，这一类群在某种意义下一般地概括了实际上存在的所有的群．

设给定某些记号 $x_\alpha, x_\beta, x_\gamma, \cdots$[1] 所组成的非空(有限或无限)集合$\mathfrak{M}$．我们约定把这些符号记作 $x_\alpha^{+1}, x_\beta^{+1}, x_\gamma^{+1}, \cdots$，并且认为，这些符号和某些新的符号 $x_\alpha^{-1}, x_\beta^{-1}, x_\gamma^{-1}, \cdots$ 是一一对应的．表示式

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \cdots x_{\alpha_n}^{\varepsilon_n} \quad (\varepsilon_i = \pm 1, i = 1, 2, \cdots, n), \tag{1}$$

即由有限多个形式如 x_α^{+1} 与 x_β^{-1} 的符号所作成的有序组(每一个符号在表示式(1)中可以重复出现)，叫做一个字，假如在表示式(1)中任何一个符号 x_α^{+1} 和它所对应的符号 x_α^{-1} 不相邻地出现．例如，$x_\alpha x_\beta^{-1} x_\alpha x_\alpha x_\gamma$, $x_\alpha x_\alpha x_\alpha x_\beta x_\alpha^{-1} x_\beta$ 都是字，而 $x_\alpha x_\beta^{-1} x_\beta x_\alpha x_\gamma$ 就不是字[2]．

数 n 叫做字 w 的长度并且用 $l(w)$ 来表示．显然，对于任意集合$\mathfrak{M}$我们可以作出任意长度的字来．长度是 1 的字就是符号 x_α 或 x_β^{-1} 本身并且只能是它们本身．我们也把一个符号也没有的空字 w_0 算作字；$l(w_0) = 0$．

---

1) 为了便于了解以下的构成法，读者可先假定集合$\mathfrak{M}$只含有两个记号 x_1 与 x_2．

2) 这里所用的字的写法不应该了解为假定有任何《乘法》的符号．字只不过是符号的一个有序组，例如我们可以把字里的符号用逗点一个一个地分开．

用我们已有的一批符号所能写出的一切字的集合，对于如下定义的运算来说作成一个群：设给定两个字

$$w_1=x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_n}^{\varepsilon_n}(\varepsilon_i=\pm1,\ i=1,2,\cdots,n),\tag{2}$$

$$w_2=x_{\beta_1}^{\delta_1}x_{\beta_2}^{\delta_2}\cdots x_{\beta_m}^{\delta_m}\quad(\delta_j=\pm1,\ j=1,2,\cdots,m),\tag{3}$$

如果等式

$$\alpha_{n-i+1}=\beta_i\text{ 且 }\varepsilon_{n-i+1}+\delta_i=0$$

对于所有的 $i(1\leqslant i\leqslant k)$ 成立，此处 k 满足条件 $0\leqslant k\leqslant\min(n,m)$，但是或者 $\alpha_{n-k}\neq\beta_{k+1}$，或者 $\alpha_{n-k}=\beta_{k+1}$ 而同时 $\varepsilon_{n-k}=\delta_{k+1}$，那末就令

$$w_1w_2=x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_{n-k}}^{\varepsilon_{n-k}}x_{\beta_{k+1}}^{\delta_{k+1}}x_{\beta_{k+2}}^{\delta_{k+2}}\cdots x_{\beta_m}^{\delta_m}.\tag{4}$$

换句话说，为了得出乘积 w_1w_2，应该把字 w_2 接在 w_1 后面，假如这样得到的表示式

$$x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_n}^{\varepsilon_n}x_{\beta_1}^{\delta_1}x_{\beta_2}^{\delta_2}\cdots x_{\beta_m}^{\delta_m}.\tag{5}$$

是字的话，即是说，如果符号 x_{α_n} 与 x_{β_1} 或者不相等，或者相等而又有相同的指数，那末就得到乘积 w_1w_2. 否则，表示式(5)中就需要进行一些缩减，就是要把所作序列中具有相反指数的一对对相同符号依次消去. 显然，在作这种缩减时，因子 w_1 与 w_2 中的一个可能完全被消掉了.

很明显，空字 w_0 在这样定义的乘法之下起着单位元的作用. 字(2)的逆元是

$$w_1^{-1}=x_{\alpha_n}^{-\varepsilon_n}\cdots x_{\alpha_2}^{-\varepsilon_2}x_{\alpha_1}^{-\varepsilon_1}.$$

特别，符号 x_α 的逆元就是符号 x_α^{-1}.

字的乘法的结合性质的证明是相当困难的. 设给定了字 w_1，w_2 及 w_3，它们都不是空字[1]. 我们利用对中间因子 w_2 的长度作归纳法来证明等式

1) 当三个因子中有一个是 w_0 时，结合律的正确性是明显的.

$$w_1(w_2w_3)=(w_1w_2)w_3 \tag{6}$$

成立.

首先考察 $l(w_2)=1$ 的情形，即 $w_2=x_\alpha^\varepsilon$. 如果字 w_1 的最后一个符号和字 w_3 的第一个符号都不等于 $x_\alpha^{-\varepsilon}$，那就不能做任何缩减，因而等式(6)成立. 如果所说的两个符号中只有一个等于 $x_\alpha^{-\varepsilon}$，这时等式(6)也成立，因为在这一情形下，乘积 w_1w_2 与 w_2w_3 之一不能再作任何缩减. 最后，如果这样的两个符号都等于 $x_\alpha^{-\varepsilon}$，那末令

$$w_1=x_{\beta_1}^{\delta_1}\cdots x_{\beta_s}^{\delta_s}x_\alpha^{-\varepsilon},\ w_3=x_\alpha^{-\varepsilon}x_{\gamma_1}^{\eta_1}\cdots x_{\gamma_t}^{\eta_t}.$$

于是表示式

$$x_{\beta_1}^{\delta_1}\cdots x_{\beta_s}^{\delta_s}x_\alpha^{-\varepsilon}x_{\gamma_1}^{\eta_1}\cdots x_{\gamma_t}^{\eta_t}$$

是一个字，因为在这个表示式里不能再作任何缩减，并且它和等式(6)的左右两端都相等.

现在设$l(w_2)\geqslant 2$. 若

$$w_2=x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_{n-1}}^{\varepsilon_{n-1}}x_{\alpha_n}^{\varepsilon_n},$$

那末令

$$w_2'=x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_{n-1}}^{\varepsilon_{n-1}}.$$

于是 w_2' 是一个字，并且 $l(w_2')<l(w_2)$而 $w_2=w_2'x_{\alpha_n}^{\varepsilon_n}$. 现在利用中间因子的长度小于 n 时的等式(6)来证明等式(6)在所考虑的情形成立:

$$\begin{aligned}w_1(w_2w_3)&=w_1[(w_2'x_{\alpha_n}^{\varepsilon_n})w_3]=w_1[w_2'(x_{\alpha_n}^{\varepsilon_n}w_3)]\\&=(w_1w_2')(x_{\alpha_n}^{\varepsilon_n}w_3)=[(w_1w_2')x_{\alpha_n}^{\varepsilon_n}]w_3\\&=[w_1(w_2'x_{\alpha_n}^{\varepsilon_n})]w_3=(w_1w_2)w_3.\end{aligned}$$

最后，在上面的等式里出现的某些括弧可能包含这样的乘积，它们只在施行缩减以后才是字. 但是这并不妨碍证明的进行.

我们现在已经有理由来谈论关于由一个已知集合$\mathfrak{M}$中的符号以及它们的逆元符号所组成的字的群了. 这个群叫做自由群. 显然，它由所给集合 $\mathfrak{M}$ 的势完全确定而不依赖于这个集合中元素的

任何个别性质．如果我们把集合$\mathfrak{M}$的势(在有限集合时，就是这个集合中元素的个数)叫做由这个集合所构成的自由群的秩，那末利用初等集合论的观点，可以证明有限秩的自由群都是可数的，而任何一个无限秩的自由群都具有和它的秩相同的势．

显然，秩是1的自由群就是无限循环群．任何一个秩大于1的自由群都是非交换的：如果$\alpha\neq\beta$，那末字$x_\alpha x_\beta$与$x_\beta x_\alpha$是这个群的不同元素．在一般情形下，除单位元外自由群的所有元素都具有无限阶：若在元素

$$w=x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\cdots x_{\alpha_n}^{\varepsilon_n}$$

中，符号$x_{\alpha_1}^{\varepsilon_1}$与$x_{\alpha_n}^{\varepsilon_n}$，符号$x_{\alpha_2}^{\varepsilon_2}$与$x_{\alpha_{n-1}}^{\varepsilon_{n-1}}$，…，符号$x_{\alpha_k}^{\varepsilon_k}$与$x_{\alpha_{n-k+1}}^{\varepsilon_{n-k+1}}$都是两两互逆的，但是对于符号$x_{\alpha_{k+1}}^{\varepsilon_{k+1}}$与$x_{\alpha_{n-k}}^{\varepsilon_{n-k}}$来说不成立，那末令

$$\overline{w}=x_{\alpha_{k+1}}^{\varepsilon_{k+1}}x_{\alpha_{k+2}}^{\varepsilon_{k+2}}\cdots x_{\alpha_{n-k}}^{\varepsilon_{n-k}}.$$

这个满足不等式$0\leqslant k<\frac{1}{2}n$的$k$一定可以找到，因为$w$不是空字。现在对于$s>0$，有

$$w^s=x_{\alpha_1}^{\varepsilon_1}\cdots x_{\alpha_k}^{\varepsilon_k}\overline{w}^s x_{\alpha_{n-k+1}}^{\varepsilon_{n-k+1}}\cdots x_{\alpha_n}^{\varepsilon_n}.$$

在这个等式右端的表示式不能再作任何缩减，这就是说，它不是一个空字．由此得出$w^s\neq1$．

我们注意，任何一个字都等于构成它的符号的乘积．因此，集合$\mathfrak{M}$是在这个集合上所建立的自由群的生成系．我们约定把自由群的这种生成系叫做它的自由生成系．以后我们对于自由群的元素将保留《字》这个名称而把它们写作生成元的幂的乘积的形式，例如不写$x_\alpha x_\alpha x_\alpha x_\beta^{-1}x_\alpha x_\beta x_\beta$而写$x_\alpha^3x_\beta^{-1}x_\alpha x_\beta^2$．

关于自由群的进一步的理论，包括许多深邃的和重要的结果，读者将在第九章里看到．现在我们来证明一个定理，这个定理完全揭示出自由群在整个群论中的意义．

任何一个群都与某一自由群的一个商群同构.

事实上，设给定任意群G并且令M是这个群的一个生成系；M中的元素用$a_\alpha, a_\beta, \cdots$来表示. 我们取这样的一个自由群$W$，它的自由生成系和$M$有相同的势. 在$M$的元素与我们所取的群$W$的自由生成系的元素之间建立一个相互单值对应，并且约定把群W的与M中a_α相对应的生成元记作x_α. 把W中的元素x_α映成它所对应的G中的元素a_α的映射，一般地，把元素

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \cdots x_{\alpha_k}^{\varepsilon_k}, \quad \varepsilon_i = \pm 1, \; i = 1, 2, \cdots, k, \tag{7}$$

映成G中等于乘积

$$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \cdots a_{\alpha_k}^{\varepsilon_k} \tag{8}$$

的元素的映射显然是群W映到整个群G上的一个同态映射。因此，根据关于同态的定理(§ 10)，推出

$$G \simeq \frac{W}{H},$$

这样就证明了这个定理. 我们注意，群W的正规子群H刚好由一切形式如(7)这样的字组成，它们所对应的乘积(8)等于群G的单位元.

由适才定理的证明中可以推出，*任何一个具有限生成元的群都是一个有限秩的自由群的商群. 说得更确切一些，任何一个具有n个生成元的群都是一个秩为n的自由群的商群.*

显然，把一个群G作为一个自由群的商群这种表示法对于这个群来说并不是唯一的，因为这种表示法依赖于集合M的选择.

设给定任意群G并且假设它被表成某一自由群W对其正规子群H的商群. 和上面一样，若$x_\alpha, x_\beta, \cdots$是群$W$的自由生成元，那末在自然同态之下，群$G$中与它们对应的元素就用$a_\alpha, a_\beta, \cdots$来表示. 而所有这种元素(自然，其中可能有相等的)的集合用$\mathfrak{M}$来表示，设字

$$x_{\alpha_1}^{s_1}x_{\alpha_2}^{s_2}\cdots x_{\alpha_k}^{s_k}(s_i \text{ 是整数})$$

是H中任意元素. 在群G中有等式

$$a_{\alpha_1}^{s_1}a_{\alpha_2}^{s_2}\cdots a_{\alpha_k}^{s_k}=1$$

与它对应,这个等式叫做集合M的元素在群G中的关系.

在H中选出这样的一个子集合$\mathfrak{N}$,使得它所生成的群W中的正规子群就是H. 与$\mathfrak{N}$中的字相对应的一组关系叫做群G的定义关系. M中的元素在G中的一切关系都可以看成定义关系的推演结果,因为H中任一元素都可以写成$\mathfrak{N}$中的元素及其共轭元素的幂积的形式.

群G由所给的定义关系完全确定,因为集合$\mathfrak{N}$在自由群W中完全确定了正规子群H,于是也就完全确定了商群$\frac{W}{H}$. 由于任意群,正如上面所证明的那样,都是一个自由群的商群,所以我们得到以下结论,任何一个群都可以由关于某一个符号集合的一组定义关系给出;因此,如果两个群由某些生成系的定义关系给出,并且在这两组生成系之间可以建立这样的一个相互单值对应,使得第一个群的定义关系可以转化为第二个群的定义关系,反过来,第二个群的定义关系也可以转化为第一个群的定义关系,那末这两个群同构.

反过来,如果给了任意一个符号的集合M及任意一组关系,这些关系把M中符号所组成的某些字和单位元等同起来,那末总可以指出这样的群,使这一组关系是它的一组定义关系. 为此,我们只需作出集合M上的一个自由群,在其中取出由这些关系左端所生成的正规子群,然后再过渡到商群就行了.

Dyck 定理 设群G是由某一组定义关系给出的,而群G'是由同样这些符号的这些关系另外再加上一些其他的关系所给出的,那末群G'与群G的一个商群同构.

事实上，如果我们使群G与G'都和同一个自由群W的两个商群同构，

$$G\simeq\frac{W}{H},\quad G'\simeq\frac{W}{H'},$$

那末正规子群H包含在正规子群H'内.

这个定理在寻求用其他方法给出的群的定义关系时往往是有用的.

例 1. n阶有限循环群是由生成元a及定义关系

$$a^n=1$$

给出的.

2. 在§7里，有理数加法群R被表示成一些无限循环群的递增序列的并集. 根据这个结果，群R可以由生成元

$$a_1, a_2, a_3, \cdots, a_n, \cdots$$

及定义关系

$$a_1=a_2^2, a_2=a_3^3, \cdots, a_n=a_{n+1}^{n+1}, \cdots$$

给出.

3. p^∞型群可以由生成元

$$a_1, a_2, \cdots, a_n, \cdots$$

及定义关系

$$a_1^p=1, a_{n+1}^p=a_n, n=1,2,\cdots$$

给出.

4. 三次对称群S_3由生成元a, b及定义关系

$$a^3=1, b^2=1, abab=1$$

给出. 事实上，元素

$$a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad b=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

生成整个群S_3并且满足关系(9)，因此(根据 Dyck 定理)群S_3是

由定义关系(9)所给出的群的商群，——群S_3由对生成元(9′)的定义关系(9)（可能还有一些其他的关系)给出．另一方面，由关系(9)得出等式$ba=a^2b$．因此，在由关系(9)所给出的群中，符号a与b的任意幂的乘积都可以利用这些关系化为$a^\alpha b^\beta$的形式，$\alpha=0,1,2,\beta=0,1$，就是说，具有定义关系(9)的群所包含的元素不能多于六个，因而与S_3重合．

5．在§9中我们已经指出，四元数群K的阶是8并且是由两个元素a,b所生成的，这两个元素由关系

$$a^4=1, b^4=1, a^2=b^2, aba=b \tag{10}$$

联系着．用同样的方法可以确定，由关系(10)所定义的群不超过八个元素．由此(再根据Dyck定理)推出，(10)是群K的一组定义关系．我们要注意，在(10)的四个关系中有两个并没有像我们以前那样来写．把这两个式子写成标准形式，在这一情形下，就是写成

$$a^2b^{-2}=1 \text{ 及 } abab^3=1,$$

是不困难的．

关于用定义关系来给出群，我们现在还要作一些补充说明，至于比较深入的问题，介绍读者在第十章里去找．我们知道，自由群是由一组自由生成元而没有任何定义关系所给出的．反过来，假如在某一个群G里可以取出一个生成系M，而这一组生成元不被任何关系所联系[1]，那末G中任意元素只能唯一地写成M中元素的字的形式，这就是说，G与以M为自由生成系的自由群同构．换句话说，在这一情形下，群G是一个自由群而M是它的一个自由生成系．

1）形式如$aa^{-1}=1$这种《自明的》关系不满足以前所给出的关系的定义，因此它不算是关系．

为使一个具有生成元 $a_\alpha, a_\beta, \cdots$ 的群是阿贝尔群，只要对于其中任意一对生成元，可以写出形式如

$$[a_\alpha, a_\beta]=1 \tag{11}$$

的定义关系就够了；在这里等式左端是元素 a_α 与 a_β 的换位元. 事实上，容易证明，由群的一切生成元之间的可换性可以推出生成元的任意两个幂积的可换性. 但是，上面所引入的例 2 和例 3 表明，如果一个群的定义关系中没有(11)那种形式的等式，它也可能是一个阿贝尔群.

任意一个群可以用各种各样的方法由生成元和定义关系来给出. 因此，尽管定义关系本身是给出群的一个很方便的《抽象》方法，也就是一般地给出所考虑的群和一切与它同构的群的方法，但是，在绝大多数情况下，用定义关系给出群很少说明问题. 比方说，如果用一组生成元和一组定义关系来给出一个群，那末常常不能确定，这个群是有限的还是无限的，它是交换的还是非交换的等等问题。不仅如此，一个群可以只由单位元这一个元素组成——当这群的定义关系左端在所对应的自由群中所生成的正规子群和整个自由群重合时，显然就有这种情况，——但是，一般来讲，这一点不能由考虑定义关系来确定. 也可能有另一个极端情形：我们的群可能实际上是一个自由群，而它却由随意一组生成元系所给出.

有限群常常不是用定义关系来给出，而是利用 Cayley 表来给出. 设有限群 G 的阶是 n，那末可以把它的元素从单位元开始加以编号:

$$1, a_2, a_3, \cdots, a_n. \tag{12}$$

然后作一个 n 行 n 列的正方形表，用符号(12)从上向下记出它的行，从左向右记出它的列，而在用 a_i 记出的行与用 a_j 记出的列的交点位置上放置等于乘积 a_ia_j 的元素. 比方说，如果我们选取三

次对称群，即具有生成元 a 和 b 以及定义关系 $a^3=1, b^2=1, abab=1$ 的群(参看前面例 4)，并且引用记法：

$$a_2=a, a_3=a^2, a_4=b, a_5=ab, a_6=a^2b,$$

那末 Cayley 表就是

	1	a_2	a_3	a_4	a_5	a_6
1	1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_3	1	a_5	a_6	a_4
a_3	a_3	1	a_2	a_6	a_4	a_5
a_4	a_4	a_6	a_5	1	a_3	a_2
a_5	a_5	a_4	a_6	a_2	1	a_3
a_6	a_6	a_5	a_4	a_3	a_2	a_1

作为两个二阶循环群直积的四阶非循环阿贝尔群，可由生成元 a, b 及定义关系

$$a^2=1, b^2=1, ab=ba$$

给出，这个群也可以用以下的 Cayley 表给出：

	1	a_2	a_3	a_4
1	1	a_2	a_3	a_4
a_2	a_2	1	a_4	a_3
a_3	a_3	a_4	1	a_2
a_4	a_4	a_3	a_2	1

一般，阿贝尔群并且只有阿贝尔群才具有关于主对角线对称的 Cayley 表。

第二篇 阿贝尔群

第六章 阿贝尔群理论基础

§19. 阿贝尔群的秩·自由阿贝尔群

阿贝尔群是最重要的几类群之一，它们的理论已经研究得相当好. 本章中将要叙述阿贝尔群理论中的一些基本概念和事实，包括具有限多个生成元的阿贝尔群的理论. 在讨论阿贝尔群理论中几个比较深入分支的以下两章中，这些概念和事实有很重要的用处.

在这一章里，以及此后凡属叙述专门和阿贝尔群有关问题的地方，我们约定采用加法术语来代替乘法术语. 由于这一约定而引起的术语和记号上的主要改变，在§3的末尾处已经指出过. 这里我们还要补充指出，群的单位子群现在应该说成*零子群*，这个子群用记号O来表示. 群中子集的乘积现在应该说成它们的*和*，并且由于阿贝尔群中所有子群都是它里面的正规子群，因而彼此可换，故阿贝尔群中两个任意子群，或一般地任何有限多个任意子群的和仍是这个群里的子群(参看§8). 最后，还应当注意，采用加法术语时，代替阿贝尔群的直积(参看§17)，我们将说它们的*直和*. 直和这个概念对讨论阿贝尔群的各章是一个基本概念.

根据§3中所引入的一般术语，如果一个阿贝尔群中所有元素的阶都是有限的，那末它就称为一个*周期阿贝尔群*；如果除去零之外所有元素都有无限阶，那末这个群就称为*无扭阿贝尔群*；如果它既含有限阶元素也包含无限阶元素，那末它就称为*混合阿贝*

尔群.

如果G是一个混合阿贝尔群，F是它里面所有有限阶元素的集合，则F显然是群G的一个子群. 这个唯一确定的子群称为群G的最大周期子群，或简称为群G的周期部分. 商群$\frac{G}{F}$是一个无扭群. 因此，任何一个混合阿贝尔群都是一个周期群——它的周期部分——借助于一个无扭阿贝尔群的扩张(参看§10).

特别，所有元素都以某一固定素数p的幂为阶的那种阿贝尔群，都是周期阿贝尔群. 这种群称为对素数p的准素阿贝尔群.

任何一个周期阿贝尔群都能分解成为一些对不同素数的准素群的直和，并且这种分解是唯一的.

事实上，群G中阶为素数p的幂的那些元素的全体是G里的一个子群，这个子群我们记作G_p; 子群G_p是G里的一个特征子群，甚至还是一个全特征子群. 对不同p的所有子群G_p构成群G里的一个直和，因为除某一G_p外所有其余这种子群的和中，元素的阶都和p互素，因而这个和与G_p的交只包含一个零元素. 在另一方面，群G中任何一个元素都包含在所有子群G_p的和之内，因为在§17中我们证明了任何一个有限循环群都可以分解成为一些准素循环群的直和.

现在我们引入阿贝尔群G的秩这个概念.

我们把群G的一个有限元素系$v_1, v_2, \cdots v_k$称为线性相关的，如果存在一组不全为零的整数$\alpha_1, \alpha_2, \cdots, \alpha_k$使等式

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$$

成立，这里等式右端的零当然是群G的零元素. 不具有这一性质的元素系称为线性无关的. 我们约定称群G中的元素u和这个群中的元素系$u', u'', \cdots, u^{(s)}$线性相关，如果这个元素的某个倍元αu, $\alpha \neq 0$, 包含在子群$\{u', u'', \cdots, u^{(s)}\}$内，也就是说，如果存在这样一

组整数 $\beta_1, \beta_2, \cdots, \beta_s$ 使

$$\alpha u = \beta_1 u' + \beta_2 u'' + \cdots + \beta_s u^{(s)}.$$

显然，元素系 $v_1, v_2, \cdots, v_k$ 是一个线性相关系，当且仅当元素 v_i 当中至少有一个元素和这个元素系中其余元素线性相关.

线性相关的下述几个性质是很明显的:

任何一个元素系，如果它包含一个有限阶元素，特别如果它包含零元素的话，一定是一个线性相关系. 线性无关系的任何一个子系也是线性无关的. 一个有限元素系中的每个元素和这个元素系线性相关.

群 G 中的两个元素系 $u', u'', \cdots, u^{(s)}$ 和 $v', v'', \cdots, v^{(t)}$ 称为等价的，如果第一个元素系中的每个元素都和第二个元素系线性相关，第二个元素系中的每个元素都和第一个元素系线性相关. 群 G 中的任何一个元素，如果它和这两个元素系之一线性相关的话，必定也和另外一个线性相关. 事实上，如果在 $\alpha \neq 0$ 时

$$\alpha u \in \{u', u'', \cdots, u^{(s)}\},$$

且在 $\beta_i \neq 0 (i = 1, 2, \cdots, s)$ 时

$$\beta_i u^{(i)} \in \{v', v'', \cdots, v^{(t)}\}$$

的话，那末元素 $(\alpha\beta_1\beta_2\cdots\beta_s)u$ 就包含在子群 $\{v', v'', \cdots v^{(t)}\}$ 内. 由这个事实可以看出，元素系的等价关系是传递的.

替换定理. 设已知群 G 的两个有限元素系

$$u', u'', \cdots, u^{(k)}, \qquad \text{(I)}$$

$$v', v'', \cdots, v^{(l)}, \qquad \text{(II)}$$

其中第一个元素系是线性无关的，并且它的每个元素都和第二个元素系线性相关. 那末我们可以断定 $k \leqslant l$，并且从元素系 (II) 中可以适当地去掉 k 个元素，使余下的元素和 (I) 的元素一道组成一个和元素系 (II) 等价的元素系.

证明. 当 $k=0$ 时这个定理显然是正确的. 现在假设它对 $k-1$

已经证明.

元素系(I)的子系 $u', u'', \cdots, u^{(k-1)}$ 也是一个线性无关系，它的每一个元素都和元素系(II)线性相关. 因此，适当地变动一下(II)中元素的号码之后，我们可以得出一个和(II)等价的元素系.

$$u', u'', \cdots, u^{(k-1)}, v^{(k)} \cdots, v^{(l)} \qquad \text{(III)}$$

元素 $u^{(k)}$ 既然和元素系(II)线性相关，也应当和元素系(III)线性相关. 这就是说，存在这样一组系数 $\alpha, \beta_1, \beta_2, \cdots, \beta_l, \alpha \neq 0$，使

$$\alpha u^{(k)} = \beta_1 u' + \beta_2 u'' + \cdots + \beta_{k-1} u^{(k-1)} + \beta_k v^{(k)} + \cdots + \beta_l v^{(l)}.$$

从这里就可以知道 $l \geqslant k$，因为系数 $\beta_k, \cdots, \beta_l$ 当中至少有一个不等于零，不然的话，元素 $u^{(k)}$ 就会和元素系 $u', u'', \cdots, u^{(k-1)}$ 线性相关了. 假设 $\beta_k \neq 0$. 这样一来，就有

$$\beta_k v^{(k)} = (-\beta_1) u' + \cdots + (-\beta_{k-1}) u^{(k-1)} + \alpha u^k + \\ + (-\beta_{k+1}) v^{(k+1)} + \cdots + (-\beta_l) v^{(l)},$$

这就是说，元素 $v^{(k)}$ 和元素系

$$u', u'', \cdots, u^{(k-1)}, u^{(k)}, v^{(k+1)}, \cdots, v^{(l)} \qquad \text{(IV)}$$

线性相关. 元素系(III)和(IV)等价，因而元素系(II)和(IV)也等价. 这样我们就证明了定理.

由替换定理可以看出，群 G 中两个等价的线性无关元素系必由同样数目的元素组成.

线性相关这个概念，可用下面的方法推广到无限元素系的情形去：阿贝尔群 G 中的一个无限元素系称为线性相关的，如果它至少包含一个线性相关的有限子系；如果它所有的有限子系都是线性无关的，那末这个元素系也就称为线性无关的. 与此相当，我们说一个元素和某一个无限元素系线性相关，如果它在上面所讲的意义下和这个元素系的某一个有限子系线性相关. 因为群 G 中一个递增的线性无关元素系序列的并集还是一个线性无关的元素系，故任何一个群 G，如果它不是周期群的话，必定有一个极大的

线性无关系，并且它里面的任何一个线性无关系都可以被嵌进一个极大线性无关系里去．如果群G是周期群的话，那末它就不可能包含任何线性无关系．

如果群G具有有限的极大线性无关系的话，那末所有这些元素系都彼此等价，因而如以上所证，都由同样数目的元素组成．这个数目称为群G的秩，而群G则称为*有限秩群*．可以把所有周期群的秩看作等于零，很自然地把它们归进有限秩群里去．不具有限秩的群，称为*无限秩群*．在这个情形，所谓群的秩，是指这个群里一个极大线性无关系的势．这个势等于群对其周期部分的商群的势，因而也是一个不变量．

有限秩群G的任何一个子群A和商群$\frac{G}{A}$也都是有限秩群，并且这两个群的秩的和等于群G的秩．

第一个断语可由这样的一个事实得出，即子群A里的任何一个线性无关元素系同时也是群G里的一个线性无关元素系．

从群$\frac{G}{A}$中任意取出一个线性无关元素（对A的陪集）系，并从这些陪集中各取出一个代表元，我们就可以得出群G里的一个线性无关元素系，由这个事实即可得出第二个断语．

为了证明第三个断语，我们从子群A中取一个极大线性无关元素系

$$a_1, a_2, \cdots, a_k, \qquad k \geqslant 0, \tag{1}$$

从商群$\frac{G}{A}$中取一个极大线性无关元素系

$$b_1+A, b_2+A, \cdots, b_l+A, \quad l \geqslant 0, \tag{2}$$

其中

$$b_1, b_2, \cdots, b_l$$

是这些陪集的任意一组代表元．这样一来，群G中的元素系

$$a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_l \tag{3}$$

将是线性无关的. 事实上，作群G对A的商群时，由等式

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k + \beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_l b_l = 0 \tag{4}$$

可得出等式

$$\beta_1(b_1 + A) + \beta_2(b_2 + A) + \cdots + \beta_l(b_l + A) = 0.$$

由于元素系(2)是线性无关的，从这里可得出

$$\beta_1 = \beta_2 = \cdots = \beta_l = 0.$$

这样一来，等式(4)就化成等式

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k = 0,$$

由于元素系(1)是线性无关的，从这里可得出

$$\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0.$$

余下来的只要证明元素系(3)是群G中的一个极大线性无关系就行了. 如果g是群G中一个任意元素，则陪集$g+A$将和元素系(2)线性相关

$$\alpha(g + A) = \gamma_1(b_1 + A) + \gamma_2(b_2 + A) + \cdots + \gamma_l(b_l + A),$$

由此即有

$$\alpha g = a + \gamma_1 b_1 + \gamma_2 b_2 + \cdots + \gamma_l b_l,$$

其中a是子群A中的一个元素，$\alpha \neq 0$. 但元素a本身又和元素系(1)线性相关:

$$\beta a = \delta_1 a_1 + \delta_2 a_2 + \cdots + \delta_k a_k,$$

而$\beta \neq 0$，故

$$(\alpha\beta) g = \delta_1 a_1 + \delta_2 a_2 + \cdots + \delta_k a_k + (\beta\gamma_1) b_1 + (\beta\gamma_2) b_2 + \\ + \cdots + (\beta\gamma_l) b_l,$$

这正好是我们所要证明的.

由上面所证明的定理可以看出，混合群的秩等于这个群对它的周期部分的商群的秩；还可以看出，有限多个有限秩群的直和还是一个有限秩群，它的秩等于各个被加群的秩的和.

现在我们研究一种特殊的阿贝尔群，这种群在阿贝尔群的整个理论中起着非常重要的作用.

有限多个或无限多个无限循环群的直和称为一个*自由阿贝尔群*. 如果

$$U=\sum_{\nu}\{u_{\nu}\}$$

是将自由阿贝尔群U分解成无限多个循环群的直和分解，则这些直被加群的生成元 u_{ν} 的全体（从每个被加群中各取一个生成元）称为群U的一个*基*. 因此，群U中的任何一个元素，都能写成基中有限多个元素以整数为系数的和.

一般说来，一个自由阿贝尔群U可以用许多种不同的方式分解成无限循环群的直和，因而具有许多个不同的基. 这样，如果群U的一个基中有元素 $u_1, u_2, \cdots$，那末可以把 u_1 换成元素 $u_1+\alpha u_2$ (α 是一个任意整数)，而把这个基变成另外一个基. 群U的基的这样一种变换，在下面一节里我们将要用到，而不再作补充说明。

自由阿贝尔群是无扭群，它的任何一个基都是它里面的极大线性无关系. 根据前面所得出的结果，从这里可以看出，*如果自由阿贝尔群U有有限秩 n 的话，那末它所有的基都由 n 个元素组成*，也就是说，任何一个将群 U 分解成无限循环群的直和分解都由 n 个被加群组成. 如果群U的秩是无限的，则它的任何一个基的势等于整个群的势.

可注意的是，自由阿贝尔群中远不是所有的极大线性无关系都能作它的基. 例如秩为 1 的自由阿贝尔群，即无限循环群$\{u\}$只有两个基——元素 u 或元素 $-u$，而这个群里的任何一个元素，只要不等于零，都是它里面的极大线性无关系.

自由阿贝尔群在阿贝尔群理论中起着自由群在整个群论中所起的作用. 具体说：

任何一个阿贝尔群G都和一个自由阿贝尔群的商群同构，并且具n个生成元的阿贝尔群和秩为n的自由阿贝尔群的商群同构.

为了证明这个定理，我们从群G中选出一个生成系$M=(a_\alpha)$，其中α跑遍某一足标的集合，并作一个自由阿贝尔群U，它的基由与集合M中的元素a_α相互单值对应的元素u_α组成.

映射

$$k_1u_{\alpha_1}+k_2u_{\alpha_2}+\cdots+k_nu_{\alpha_n}\longrightarrow k_1a_{\alpha_1}+k_2a_{\alpha_2}+\cdots+k_na_{\alpha_n}$$

显然是群U到群G上的一个同态映射. 因此，根据同态定理(§ 10)，群G和群U对子群V的商群同构，而子群V则由群U中被这个映射映到群G的零元的那些元素所组成:

$$G\simeq\frac{U}{V}.$$

自由阿贝尔群的任何一个非零子群也是自由阿贝尔群[1].

设V是自由阿贝尔群U的一个子群. 假设群U的基已经良序化:

$$a_1, a_2, \cdots, a_\alpha, \cdots, \alpha<\tau$$

U中任何一个元素$x, x\neq 0$，可唯一地写成下面的形式

$$x=k_1a_{\alpha_1}+k_2a_{\alpha_2}+\cdots+k_na_{\alpha_n},$$

其中$\alpha_1<\alpha_2<\cdots<\alpha_n$，所有$k_i$都不等于零. 我们约定将$\alpha_n$称为元素$x$的末项足标，$k_n$称为它的末项系数. 试考虑$V$中具下述性质的一些元素，它们的末项足标是$V$中所有元素的末项足标中最小的，并从这些元素中选出一个元素b_1，使其具有最小的正末项系数. 很容易看出，V中的任何一个元素v，如果它的末项足标和b_1的末项足标相同的话，一定包含在循环子群$\{b_1\}$内. 事实上，我们

1) 这个定理的一个特殊情形，即关于有限秩阿贝尔群的情形，在下一节中另有一个证明.

可以把 b_1 的末项系数写作 k，把 v 的末项系数写作 l. 如果 $l=kq+r$，$0\leqslant r<k$，则 V 中的元素 $v-qb_1$(如果它不等于零的话)或者和 b_1 有相同末项足标(当 $r>0$ 时)，但末项系数比 b_1 的末项系数小，或者(当 $r=0$ 时)有较小的末项足标. 可是在两种情形下我们都得出和元素 b_1 的选择相矛盾的结论，故 $v=qb_1$.

现在假设对小于 γ 的所有 β，在子群 V 里都选出了元素 b_β，并且这些元素线性无关，也就是说，由这些元素所生成的子群 V' 是循环群 $\{b_\beta\}$ 的直和；而 V 中的任何一个元素，如果它的末项足标不大于某元素 b_β 的末项足标的话，都包含在 V' 内. 从属于 V 而不属于 V' 的元素当中，我们选出末项足标最小的那些元素，并从这些元素当中选出一个元素 b_γ，使具有最小的正末项系数. 元素 b_γ 的任何一个倍元和 b_γ 有相同的末项足标，故 $V'\cap\{b_\gamma\}=0$，由此即有

$$\{V', b_\gamma\}=V'+\{b_\gamma\}.$$

其次，如果 V 中的元素 c 和 b_γ 有相同的末项足标，且元素 b_γ 和 c 的末项系数分别是 k_γ 和 k，则(根据元素 b_γ 的定义) k 应被 k_γ 整除，$k=k_\gamma k'$. 因此，元素 $c-k'b_\gamma$ 的末项足标比元素 b_γ 的末项足标小，因而 $c-k'b_\gamma\in V'$，而 $c\in V'+\{b_\gamma\}$. 这种选择元素 b_β 的过程，可以一直继续下去，直到子群 V 的全部元素都用光为止. 因此，子群 V 是一个自由阿贝尔群，以 $b_1, b_2, \cdots, b_\beta, \cdots$，为基，其中 β 小于某一 σ.

最后，我们证明下面的定理.

如果阿贝尔群 G 对子群 B 的商群是一个自由阿贝尔群，则 B 是 G 的一个直被加子群.

事实上，设

$$\frac{G}{B}=\sum_{\alpha}\{\bar{a}_\alpha\}$$

是将群 $\frac{G}{B}$ 分解成无限循环群的一个直和分解. 从每一个陪集 $\bar{a}_\alpha$ 里

选出一个代表元 a_α. 所有元素 a_α 所生成的群 G 里的子群 A, 是循环群 $\{a_\alpha\}$ 的直和, 并且 $A\cap B=0$. 同时, 群 G 对子群 B 的任何一个陪集都包含 A 里的一个元素, 因此

$$G=\{B, A\}=B+A.$$

可注意的是, 使阿贝尔群 G 的商群为自由阿贝尔群的那些子群当中, 可能没有最小的, 因此群 G 不一定能够分解成为一个自由群和一个没有自由商群的群的直和. 可数多个无限循环群的全直和(参看 § 17)就是这类群的一个例子.

§ 20. 具有限多个生成元的阿贝尔群

具有限多个生成元的阿贝尔群, 是已作了彻底研究的一类群. 这种群的意义在于他们在各种应用中有着非常重要的作用. 例如在组合拓扑学中具有限多个生成元的阿贝尔群就是一个主要工具.

从前面一节中我们已经知道, 具 n 个生成元的阿贝尔群是 n 秩自由阿贝尔群的一个商群. 在这一节里, 我们用 U_n 来表示这个自由阿贝尔群. 其次, 我们还知道, 群 U_n 的任何一个子群也是自由阿贝尔群, 它的秩当然不大于 n. 现在我们不利用最后所讲的这个结果, 而证明下面这个关于群 U_n 的子群的更一般的定理. 具有限多个生成元的阿贝尔群的整个理论, 实质上都是建立在这个定理的基础之上的.

群 U_n 的任何一个异于 O 的子群 V 也是一个自由群, 它的秩 k 不大于 n; 并且还可以选择群 U_n 的一个基 $\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_n$ 和群 V 的一个基 $v_1, v_2, \cdots, v_k$, 使

$$v_i=\varepsilon_i\bar{u}_i, \quad i=1, 2, \cdots, k,$$

其中 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$ 都是正整数, 并且 ε_{i+1} 能被 ε_i 整除, $i=1, 2, \cdots, k-1$.

证明：从循环群的子群定理（§6）直接可以看出这个定理对 $n=1$ 正确. 假设这个定理对 U_{n-1} 已经证明. 如果在群 U_n 里给出了一个异于 O 的子群 V，则任意选定群 U_n 的一个基之后，总可以找到一个正整数和这个基相对应；这就是作为系数出现于组成 V 的那些线性形式（对这个选定的基）中的最小正整数. 当群 U_n 的基改变时，这个最小正系数一般也是会跟着改变的. 现在我们找出群 U_n 的一个基，使这系数取值最小. 设这个基是

$$u_1, u_2, \cdots, u_n, \tag{1}$$

设 $\varepsilon_1(\varepsilon_1\geqslant 1)$ 是和这个基相对应的最小正系数，并设

$$v_1=\varepsilon_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n$$

是子群 V 中含 ε_1 作为其表达式中的一个系数的元素之一.[1]

用 ε_1 去除系数 $\alpha_2, \alpha_3, \cdots, \alpha_n$ 得

$$\alpha_i=\varepsilon_1 q_i+r_i, \quad 0\leqslant r_i<\varepsilon_1, \quad i=2, 3, \cdots, n.$$

并将元素 u_1 换成元素

$$\bar{u}_1=u_1+q_2 u_2+\cdots+q_n u_n$$

而作基(1)的一个变换. 对新的基

$$\bar{u}_1, u_2, \cdots, u_n$$

元素 v_1 可写成下面的形式

$$v_1=\varepsilon_1\bar{u}_1+r_2 u_2+\cdots+r_n u_n,$$

因为所有 $r_i, i=2, \cdots, n$，都是小于 ε_1 的非负整数，故根据 ε_1 的选择可知

$$r_2=r_3=\cdots=r_n=0,$$

也就是说

$$v_1=\varepsilon_1\bar{u}_1.$$

我们把子群 V 中对新基表成线性形式时 $\bar{u}_1$ 的系数为零的元

1) 假定 ε_1 是 u_1 的系数是可以的，因为我们并不把 U_n 的基看作已排定次序.

素集合在一起. 这些元素组成V的一个子群V'，这个子群和元素v_1所生成的循环子群的交等于O. 兹证明子群$\{v_1\}$和V'的和等于V. 设

$$v=\beta_1\bar{u}_1+\beta_2u_2+\cdots+\beta_nu_n$$

是子群V中任意一个元素. 如果$\beta_1=\varepsilon_1q+r, 0\leqslant r<\varepsilon_1$, 则$V$中的元素

$$v'=v-qv_1=r\bar{u}_1+\beta_2u_2+\cdots+\beta_nu_n$$

以一个较ε_1为小的非负整数r为$\bar{u}_1$的系数；由此根据ε_1的定义可知$r=0$. 因此元素v'包含在子群V'内,而元素

$$v=qv_1+v'$$

包含在子群$\{v_1\}$与V'的和内.

由此可知,如果$V'=O$, 则$V=\{v_1\}$，这样我们的定理就被证明了. 如果V'不等于O,我们就得出子群V的一个直分解

$$V=\{v_1\}+V'.$$

子群V'包含在子群$U'=\{u_2, \cdots, u_n\}$内，而后者是一个$n-1$秩的自由阿贝尔群，因此根据归纳假定V'是一个自由阿贝尔群. 其次，还存在U'的这样一个基$\bar{u}_2, \cdots, \bar{u}_n$和$V'$的一个基$v_2, \cdots, v_k$，对于它们,$k-1\leqslant n-1$,且$v_i=\varepsilon_i\bar{u}_i$,其中$\varepsilon_i>0, \varepsilon_{i+1}$可被$\varepsilon_i$整除,$i=2, 3, \cdots, k$.

我们已经证明了子群V是一个k秩自由群,$k\leqslant n$[1]. 要证明群U_n的基

$$\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_n \tag{2}$$

和群V的基

$$v_1, v_2, \cdots, v_k \tag{3}$$

满足定理中的全部要求,我们只要证明ε_2能被ε_1整除就行了. 设

1) 自由群的一个真子群的秩可能和这个群本身的秩相等.

$\varepsilon_2=\varepsilon_1 q_0+r_0$，$0\leqslant r_0<\varepsilon_1$. 将元素 $\bar{u}_1$ 换成元素

$$\bar{u}'_1=\bar{u}_1-q_0\bar{u}_2$$

而作群 U_n 的基(2)的变换. 对这个新的基，V 中的元素 v_2-v_1 可写成下面的形式

$$v_2-v_1=(-\varepsilon_1)\bar{u}'_1+r_0\bar{u}_2,$$

由此再根据 ε_1 的定义可知 $r_0=0$.

这样，群 U_n 的子群定理就被完全证明了. 直接运用这个定理可证明下面的基本定理.

任何一个具有限多个生成元的阿贝尔群可分解成循环群的直和[1].

证明. 设已知一个具有限多个生成元的阿贝尔群 G. 我们知道，群 G 和一个自由群 U_n 对它的一个子群 V 的商群同构. 根据上面所证明的定理我们可以选取 U_n 的一个基 $u_1, u_2, \cdots, u_n$ 和 V 的一个基 $v_1, v_2, \cdots, v_k$，使在 $i=1, 2, \cdots, k$ 时，$v_i=\varepsilon_i u_i$，其中 $\varepsilon_i>0$，ε_{i+1} 可被 ε_i 整除. 由于基的这样一种选择法，群 U_n 中的元素

$$u=\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n \tag{4}$$

包含在子群 V 内，当且仅当系数 $\alpha_i(i=1, 2, \cdots, k)$ 可被 ε_i 整除，而系数 $\alpha_j(j=k+1, \cdots, n)$ 等于零. 事实上，如果 u 的系数满足这两个条件，则 u 可通过基 $v_1, v_2, \cdots, v_k$ 写出；反之，如果

$$u=\beta_1 v_1+\beta_2 v_2+\cdots+\beta_k v_k$$

的话，那末只要将每个 v_i 换成 $\varepsilon_i u_i$ 并和(4)进行比较就行了，因为 U_n 里的任何一个元素都是可以通过这个群的基唯一地写出的. 商群 $\frac{U_n}{V}$ 中的元素 u_i+V 在 $i\leqslant k$ 时以 ε_i 为阶；而在 $i>k$ 时则有无限阶. 所有这些元素的循环群的和等于整个商群；并且根据上面

1) 如果这个阿贝尔群是一个循环群的话，这个直分解当然也只能由一个直被加群组成.

所作的按语，这个和甚至还是一个直和——$\frac{U_n}{V}$中的任何一个元素可以唯一地写成循环群 $\{u_i+V\}$ 中的元素的和．当然，如果整数 $\varepsilon_1, \varepsilon_2, \cdots$ 当中头几个等于 1 的话，那末相应的直被加群$\{u_1+V\}$，$\{u_2+V\}$，…应该剔除掉．因为群G和商群$\frac{U_n}{V}$同构，故我们不仅对$\frac{U_n}{V}$，而且也对G证明了这定理．

特别，从这个定理可以看出，任何一个具有限多个生成元的非循环阿贝尔群都是可分解的．从§17 中我们知道，无限循环群以及任何一个准素循环群——即 p^m 阶循环群，p 是素数——都是不可分解的；另一方面，一个非准素有限循环群可分解成为一些准素循环群的直和．利用最后这个结果，可以将基本定理的表述改进如下：

任何一个具有限多个生成元的阿贝尔群可分解成有限多个不可分解的循环子群的直和，这些循环群中一部分是有限准素群，一部分是无限循环群．

当群G被分解成不可分解子群的直和时，直被加循环群中的生成元(每一被加群中取一个生成元)组成G的一个基．在自由群的情形，这个概念和前节中所定义的基的概念相吻合．

特别，从上面所证的基本定理可以看出，任何一个有限阿贝尔群可分解成一些有限循环群的直和，这些有限循环群甚至还可以认为是准素的．阿贝尔群理论的创立正是从这个定理开始．这个定理 Gauss 早就已经部分地知道了，第一个完全的证明是劳必 Frobenius 和 Stickelberger [1] 给出的．后来这个定理曾经多次被反复证明过；对具有限多个生成元的无限阿贝尔群的情形，基本定理也有好几个证法．[参看补充 28.2.]

这样，如果我们取一切可能的循环群(无限循环群或有限准素

循环群)的有限系作直和，我们就可以得出所有具有限多个生成元的阿贝尔群. 这样得出的所有阿贝尔群是否互不相同呢？下面的定理对这个问题给出了一个肯定的回答.

当一个具有限多个生成元的阿贝尔群被分解成不可分解的子群的直和时，这个分解式中被加无限循环群的数目和被加准素循环群的阶的全体和分解的方式无关，也就是说，与它的基的选择无关.

换句话说，将群 G 表为不可分解的循环群的直和的任意两个直分解彼此同构.

这个定理的证明，我们将结合着群 G 的子群定理(以下就要讲到)的证明一道给出. 现在先证明下面一个断语:

具有限多个生成元的阿贝尔群 G 的任何一个子群 H 也是具有限生成系的.

事实上，群 G 是一个自由阿贝尔群 U 对其子群 V 的商群. 子群 H 对应于群 U 中一个包含 V 的子群 U'，并且

$$H \simeq \frac{U'}{V}.$$

但如前面所证，子群 U' 有一个有限生成系，故子群 H 也有一个有限生成系.

具有限多个生成元的阿贝尔群 G 的子群定理如下:

设某一个将群 G 分成不可分解循环群的直和分解中有 r 个被加无限循环群，$r \geqslant 0$；其次，设属于固定素数 p 的被加准素循环群的数目是 k_p，且 $k_p \geqslant 0$，而这些被加群的阶是

$$p^{\alpha_{p1}}, p^{\alpha_{p2}}, \cdots, p^{\alpha_{pk_p}},$$

其中

$$\alpha_{p1} \geqslant \alpha_{p2} \geqslant \cdots \geqslant \alpha_{pk_p}.$$

另一方面，设给定了一个将群 G 的子群 H 分成不可分解循环群的

任意直分解，其中包含 s 个被加无限循环群，而对每个素数 p，包含 l_p 个属于 p 的被加准素群，并设这些准素群的阶是

$$p^{\beta_{p1}}, p^{\beta_{p2}}, \cdots, p^{\beta_{pl_p}},$$

其中

$$\beta_{p1} \geqslant \beta_{p2} \geqslant \cdots \geqslant \beta_{pl_p}. \tag{5}$$

那末在这样的情形下我们将有

$$s \leqslant r, \tag{6}$$

而对每个素数 p，

$$l_p \leqslant k_p, \tag{7}$$

$$\beta_{pi} \leqslant \alpha_{pi}, \qquad i = 1, 2, \cdots, l_p. \tag{8}$$

这个定理将和群 G 的直分解的同构定理一道证明.

首先，很容易看出，出现于群 G 的一个任意选定的基中的无限阶元素构成 G 的一个极大线性无关系，因此这些元素的数目等于这个群的秩，也就是说，和基的选择无关. 从这里也可以得出子群定理中的断语(6)，因为子群 H 的秩是不会超过群 G 的秩的.

其次，我们知道，群 G 的周期部分 A 可分解成对不同素数的准素群的直和，

$$A = \sum_p A_p$$

而子群 H 的周期部分则可分解为它和子群 A_p 的交 $B_p = H \cap A_p$ 的直和. 同时，还很容易验证，子群 A_p 由群 G 的任意一个基中阶为素数 p 的幂的那些元素生成. 这样一来，两个定理的证明都归结于有限准素群 A_p 及其子群 B_p 的情形.

我们先给出关于子群定理的证明. 由群 A_p 中 p 阶元素所构成的子群是 k_p 个 p 阶循环群的直和，就是说，它的阶等于 p^{k_p}. 群 B_p 中相应子群的阶等于 p^{l_p}. 由此即有 $l_p \leqslant k_p$. 现在设

$$\beta_{p1} \leqslant \alpha_{p1}, \cdots, \beta_{p,j-1} \leqslant \alpha_{p,j-1} \quad 但 \ \beta_{pj} > \alpha_{pj} \tag{9}$$

群 A_p 中可被数 $p^{\alpha_{pj}}$ 在这个群内整除的元素，也就是使方程

$$p^{\alpha_{pj}}x=c$$

在 A_p 内有解的元素 c 的全体 C，是群 A_p 里的一个子群. 如果 a_1, $a_2, \cdots, a_{k_p}$是群A_p 的已给基，且元素a_i 的阶是$p^{\alpha_{pi}}(i=1, 2, \cdots, k_p)$，那末不难验证，子群$C$ 将是由元素

$$p^{\alpha_{pj}}a_1, p^{\alpha_{pj}}a_2, \cdots, p^{\alpha_{pj}}a_{j-1},$$

所生成的循环群的直和，也就是说，C 有一个由 $j-1$ 个元素所组成的基. 另一方面，由于(9)和(5)，子群 B_p 中能被 $p^{\alpha_{pj}}$ 在 B_p 内整除的元素所组成的子群 C'，有一个含不少于 j 个元素的基. 但 C' 是 C 里的子群，而我们已经证明了(7)，即证明了有限准素群的子群的基中元素的个数不能大于整个群的基中元素的个数，这就是一个矛盾. 所得出的这个矛盾就结束了子群定理的证明.

群 A_p 的直分解的同构定理可由子群定理直接引出：我们可以命 $B_p=A_p$，并注意对群 A_p 的这两个基，除不等式(7)和(8)之外，由于对称性之故，反向的不等式也成立. 即有

$$l_p=k_p,$$

$$\beta_{pi}=\alpha_{pi}\quad i=1, 2, \cdots, l_p.$$

具有限多个生成元的阿贝尔群的任意一个直分解中，被加无限循环群的个数——群的秩——和被加准素循环群的阶，称为这个群的不变量. 这组不变量甚至还是一组全不变量，因为任意两个群，如果它们的这两类不变量相同的话，必定同构. 利用这些数的不变性，读者不难证明，证明基本定理时所得出的那种直分解里，作为被加循环群的阶的那一组一个相继整除另外一个的整数 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$ 也是不变的，也就是说，这组数和群的直分解的选择无关. 这些数有时称为群 G 的扭系数；为简便起见，被加准素循环群的阶我们称为群 G 的有限不变量.

在子群定理里我们对具有限多个生成元的阿贝尔群的子群的

不变量作出了一个描述，这当然还不能回答就这一类子群所能提出的全部问题. 例如有许多数学家就曾研究过有限阿贝尔群所有子群的数目，或某种特殊类型的子群的数目的问题. 在这方面有下面一个问题：如果用一组不变量给定了一个有限准素群，并选定了这个群的一个基，能不能给它的每个子群以某种“标准”基，而把它们全部列举出来？子群的标准基在整个群的基的选定之后应该是唯一地确定的，并且在某种意义上是最好的. 在 Birkhoff 的工作[3]里，给出了这个问题的解答.

§ 21. 阿贝尔群的自同态环

对于阿贝尔群 G 的自同态，除我们在 § 12 中所知道的乘法之外，还可以引入加法. 具体说，自同态 χ 和 η 的和，指的是将群 G 中的任意元素 a 映成元素 $a\chi+a\eta$ 的映射：

$$a(\chi+\eta)=a\chi+a\eta.$$

这个映射也是群 G 的自同态，因为

$$(a+b)(\chi+\eta)=(a+b)\chi+(a+b)\eta=(a\chi+b\chi)+$$
$$+(a\eta+b\eta)=a(\chi+\eta)+b(\chi+\eta)^{1)}.$$

自同态的加法满足交换律和结合律. 零自同态起着零的作用. 如果 χ 是群 G 的一个自同态，则将这个群中的每个元素 a 映成元素 $-a\chi$ 的映射 $-\chi$：

$$a(-\chi)=-a\chi$$

也是一个自同态.

$$(a+b)(-\chi)=-(a+b)\chi=-(a\chi+b\chi)=$$
$$=a(-\chi)+b(-\chi),$$

1) 这里我们要用到群 G 中运算的交换性. 在 G 为非阿贝尔群的情形，自同态 χ 和 η 的和仍是自同态的充分必要条件，是子群 $G\chi$ 和 $G\eta$——群 G 在这两个映射下的象——按元素可换，在这样的情形，χ 和 η 称为可加的.

且自同态 χ 和 $-\chi$ 的和等于零自同态. 这样一来，自同态的减法也可以实施:

$$\chi-\eta=\chi+(-\eta).$$

阿贝尔群的自同态的和与积由分配律联结起来:

$$(\chi_1+\chi_2)\eta=\chi_1\eta+\chi_2\eta, \tag{1}$$

$$\eta(\chi_1+\chi_2)=\eta\chi_1+\eta\chi_2. \tag{2}$$

事实上，对于 G 中任意元素 a,

$$a[(\chi_1+\chi_2)\eta]=[a(\chi_1+\chi_2)]\eta=(a\chi_1+a\chi_2)\eta=$$
$$=(a\chi_1)\eta+(a\chi_2)\eta=a(\chi_1\eta)+a(\chi_2\eta)=$$
$$=a(\chi_1\eta+\chi_2\eta),$$

这就证明了等式(1). 也可以同样简单地证明等式(2).

以上所说的一切，和§12中所得到的关于自同态的乘法的结果结合起来，就得出了下面的定理:

阿贝尔群全部自同态的集合，对自同态的加法和乘法构成一个环.

非交换群的自同态不能构成一个环，因为不能不受限制地进行加法和减法. 讨论非交换群的自同态的性质的，有 Fitting 的工作[1, 4].

现在让我们来看几个例子，先求出无限循环群的自同态环. 设 a 是这个群的生成元. 自同态 χ 将元素 a 映成一个元素 na ($n\gtreqless 0$)，并且 n 一经给定之后，自同态 χ 就被完全决定. 这样一来，在无限循环群的自同态和整数之间就建立了一个相互单值的对应. 如果

$$a\chi=na, \quad a\eta=ka,$$

则

$$a(\chi\eta)=(na)\eta=(nk)a,$$

$$a(\chi+\eta)=na+ka=(n+k)a.$$

这样我们就得到：无限循环群的自同态环和整数环C同构．用同样的方法可以证明，n阶有限循环群的自同态环和环C对模n的剩余环C_n同构．

现在我们来求有理数加法群R的自同态环．这个群的任何一个自同态χ由数1的象所完全决定：如果$1\chi=r$，而$\left(\frac{1}{n}\right)\chi=r'$，则$nr'=\left(n\cdot\frac{1}{n}\right)\chi=r$，从而$r'=\frac{r}{n}$，因此

$$\left(\frac{m}{n}\right)\chi=\frac{m}{n}r. \tag{3}$$

反之，任意取一个有理数r并用公式(3)来定义一个映射χ，我们就可以得出群R的一个自同态．这样一来，我们就在群R的自同态和有理数之间建立了一个相互单值的对应，而因为由

$$1\cdot\chi=r_1,\quad 1\cdot\eta=r_2$$

可得出

$$1\cdot(\chi\eta)=r_1\eta=r_1r_2$$
$$1\cdot(\chi+\eta)=r_1+r_2,$$

故群R的自同态环和有理数域同构．因此，群R的任何一个非零的自同态都有逆，因而是一个自同构．

最后，我们求p^∞型群的自同态环．这个群可由生成元

$$a_1, a_2, \cdots a_n, \cdots \tag{4}$$

和定义关系

$$pa_1=0,\quad pa_{n+1}=a_n\ n=1,2,\cdots \tag{5}$$

来决定．给出(4)中所有元素的象之后，这个群的自同态χ就可以唯一地决定．另一方面，因为这个群中阶不大于p^n的元素都包含在子群$\{a_n\}$内，故

$$a_n\chi=k_na_n,\quad n=1,2,\cdots, \tag{6}$$

其中

$$0 \leqslant k_n < p^n. \tag{7}$$

其次，因为对(4)中元素的象来说关系(5)也应该成立，故

$$p(a_{n+1}\chi) = a_n\chi,$$

从而

$$p(k_{n+1}a_{n+1}) = k_{n+1}a_n = k_n a_n,$$

这就是说，

$$k_{n+1} \equiv k_n (\mathrm{mod}\, p^n), \quad n = 1, 2, \cdots. \tag{8}$$

因此，对 p^∞ 型群的任何一个自同态 χ，都有一个适合条件(7)和(8)的自然数列

$$(k_1, k_2, \cdots, k_n, \cdots) \tag{9}$$

与之对应. 和不同自同态相对应的自然数列也互不相同，因为至少有一个元素 a_n 在这些自同态下有不同的像. 另一方法，任何一个适合条件(7)和(8)的自然数列(9)都能决定一个自同态，即由等式(6)所决定的自同态.

设除了由自然数列(9)所决定的自同态 χ 之外，在 p^∞ 型群中还给出了另外一个自同态 η，和它相对应的自然数列是

$$(l_1, l_2, \cdots, l_n, \cdots) \tag{10}$$

在这时

$$a_n(\chi + \eta) = (k_n + l_n)a_n, \quad a_n(\chi\eta) = (k_n l_n)a_n$$

但对自然数列(9)条件(8)成立，而对数列(10)类似的条件也成立，故

$$k_{n+1} + l_{n+1} \equiv k_n + l_n (\mathrm{mod}\, p^n)$$
$$k_{n+1} l_{n+1} \equiv k_n l_n (\mathrm{mod}\, p^n),$$

并且如果在这些同余式中左端换成对模 p^{n+1} 的正余数，右端换成对模 p^n 的正余数，同余关系也不会破坏. 因此，对应于 χ 与 η 的和与积的自然数列，是将数列(9)和(10)按项相加相乘，并在第 n 位将所得结果对模 p^n 约化所得的数列.

因此，满足条件(7)和(8)的形式和(9)的自然数列的集合，加上按上述规律所进行的加法和乘法，和 p^∞ 型群的自同态环同构，因而这个集本身也是一个环，并且是交换环. 这个环称为 p-进整数环，它在代数学的许多不同分枝中，特别是在域论和拓扑代数中起着非常重要的作用. 因此，p^∞ 型群的自同态环和 p-进整数环同构.

和零自同态相对应的数列(0,0…，0,…) 是 p-进整数环中的零元，而和恒等自同态相对应的数列(1, 1,…, 1,…)则是这个环中的单位元. 其次，因为 p^∞ 型群的自同态同时是自同构的充分必要条件是它不把 a_1 映成零，故 p-进整数(9)有逆的充分必要条件是 $k_1\neq 0$.

用这方法还可以得出 p-进整数环的其他许多性质. 我们只证明，这个环不包含零因子. 事实上，p^∞ 型群在任意非零自同态下的象是这个群本身，而不是它的真子群. 因此依次施行两个非零自同态的结果，不可能是零自同态.

现在让我们转到**直和的自同态环**问题上来. 为了这个目的，必须引入将一个阿贝尔群映到另一阿贝尔群的同态映射群的概念. 试考虑将群 A 映入群 B 的所有同态的集合，并对这个集合中的任意两个同态映射 χ 和 η 用公式

$$a(\chi+\eta)=a\chi+a\eta, a\in A$$

定义它们的和.

至于映射 $\chi+\eta$ 仍旧是一个同态映射，并且用这方法把群 A 到群 B 的同态映射的集合变成一个阿贝尔群的证明，可逐句重复本节开头处对自同态的加法这个特殊情形所作的证明得出.

注意，如果给定了三个阿贝尔群 A, B 和 C，那末我们就可以讨论将 A 映入 B 的同态映射与将 B 映入 C 的同态映射的乘积，并将其了解为相继施行这两个同态映射的结果. 这个映射显然是一

个将 A 映入 C 的同态映射.

现在设阿贝尔群 G 可表成有限多个群 H_i 的直和:

$$G=\sum_{i=1}^{n}H_i,$$

我们用 R_{ii} 表示群 H_i 的自同态环，用 $R_{ij}(i\neq j)$ 表示将群 H_i 映入群 H_j 的同态映射群. 于是下面的定理成立(参看 Кищкина[1])。

群 $G=\sum_{i=1}^{n}H_i$ 的自同态环和 n 阶方阵 (χ_{ij}) 的环同构，其中 $\chi_{ij}\in R_{ij}$，矩阵加法和乘法的定义和普通的定义相同[1].

事实上，对于每一个这样的矩阵 (χ_{ij})，我们可以使一个将群 G 映入其自身的映射 χ 和它相对应，这个映射定义如下：如果 $g\in G$，且

$$g=\sum_{i=1}^{n}h_i,\qquad h_i\in H_i,$$

则命

$$g\chi=\sum_{i=1}^{n}\sum_{j=1}^{n}h_i\chi_{ij}.$$

很容易看出，这个映射是群 G 的一个自同态. 反之，群 G 的任何一个自同态 χ 都在这种意义下和一个矩阵相对应：如果 h_i 是 H_i 中的一个任意的元素，而

$$h_i\chi=\sum_{j=1}^{n}h_{ij},\qquad h_{ij}\in H_j,$$

我们可命

1) 注意，对于这样的矩阵(方阵)，不但加法可以进行(这是显而易见的)，乘法也是可以进行的，并且所得出的矩阵仍然是这样一种矩阵(方阵).

$$h_i\chi_{ij}=h_{ij};$$

映射 χ_{ij} 显然是一个将 H_i 映入 H_j 的同态映射. 要证明群 G 的自同态和 (χ_{ij}) 这种形状的矩阵之间的相互单值对应,的确,使矩阵的和与积同自同态的和与积相对应,这事并不困难,可留给读者自己去作. 特别,由此可以看出,(χ_{ij}) 这种形状的矩阵的确组成一个环.

从上面所证明的定理,和 § 12 中所得出的结果可以看出,群 $G=\sum_{i=1}^{n}H_i$ 的自同构群,和所有 (χ_{ij}) 形矩阵环中具有逆矩阵的那些矩阵所组成的乘法群同构. 注意与群 G 的恒等自同构对应的是那样一个矩阵,它的主对角线上的元素是环 R_{ii} 中的单位元,而在主对角线之外则全是零.

现在我们将这些结果应用于具有限多个生成元的阿贝尔群的情形;我们知道,这样的阿贝尔群可以分解成一些无限循环群和有限准素循环群的直和. 循环群的自同态环我们已经知道了. 同样容易证明下面的断语:如果 A 和 B 是两个循环群,无限的或有限准素的,那末将 A 映入 B 的同态映射群:1)与群 B 同构,如果 A 是无限循环群的话;2)与 $p^{\min(k,l)}$ 阶循环群同构,如果 A 和 B 都是对同一素数 p 的准素循环群,其阶分别为 p^k 和 p^l;3)在所有其余情形等于零. 其次还应注意,如果已知三个循环群 $\{a\}$、$\{b\}$ 和 $\{c\}$ 以及将第一个群映入第二个群的同态映射 φ 和将第二个群映入第三个群的同态映射 ψ,并且

$$a\varphi=kb,\quad b\psi=lc,$$

则

$$a(\varphi\psi)=(kl)c.$$

因此,如果将上述循环群的同态映射群看作整数环 C 或其相应的剩余环 C_n 的加法群,那末我们就得出,同态映射的乘积和相应的

整数的乘积相当，这个乘积当然要以群$\{c\}$的阶为模约化.

我们建议读者自己去作出上一段中各个命题的详细证明，及以不变量给出的具有限多个生成元的阿贝尔群的自同态环的实际描述. 在这里，我们只指出下述有关自由阿贝尔群情形的结果.

n秩自由阿贝尔群的自同态环，与n阶整数方阵环同构.

n秩自由阿贝尔群的自同构群，与行列式等于± 1的n阶整数方阵所组成的乘法群同构.

有一系列的论文是研究各种类型的阿贝尔群的自同构群和自同态环的，其中有 Shoda[1], [3], Baer[14], [27], Derry[1], Shiffman[1], Кишкина[1]等人的工作. [参看§补充. 34.]

§22. 带算子的阿贝尔群

在带算子阿贝尔群的各种不同的应用中，算子区通常是一个结合环R，其元素为$\alpha, \beta, \gamma, \cdots$，并且，除了对任意算子成立的条件

$$(a+b)\alpha = a\alpha + b\alpha$$

之外，下面两个条件也成立，这两个条件建立了群G中的运算和环R中的两项运算之间的关系：

$$a(\alpha+\beta) = a\alpha + a\beta \tag{1}$$

$$a(\alpha\beta) = (a\alpha)\beta^{1)} \tag{2}$$

只有在条件(1)和(2)都满足时，我们才说*群G具有算子环R*. 有时也说，群G是*环R上的一个模*，或说得简单一些，是一个R-*模*.

如果将阿贝尔群G的自同态环或它的任意一个子环看作它的算子区，则条件(1)和(2)可由自同态的和与乘积的定义直接得出，

1) 当然必须注意，等式(1)左端的+号是环R中加法的记号，而等式右端的+号则表示群G中的运算. 同样应该区别等式(2)中R的元素的乘积及R中的算子对G中元素的作用.

因此这两个条件是非常自然的. 其次，如果将一个环看作它的加法群的右侧算子区，则条件(1)和(2)即成为环中两个运算的分配律和乘法的结合律. 最后，高等代数课程中所研究的一个域P上的向量空间，显然就是一个P-模. 注意，任何一个不带算子的阿贝尔群都可以看作整数环上的模.

由(1)可知

$$a\alpha=a(\alpha+0)=a\alpha+a\cdot 0,$$

从而$a\cdot 0=0$[1]，也就是说，环R中的零元作为一个算子相当于群G的零自同态.

其次

$$a\alpha=a(\alpha+\beta-\beta)=a(\alpha-\beta)+\alpha\beta,$$

因而

$$a(\alpha-\beta)=a\alpha-a\beta. \tag{1'}$$

如果环R具有单位元ε的话，则与算子ε相对应的不一定是群G的恒等自同构. 例如，如果对G中的任意a和R中的任意α我们命$a\alpha=0$的话，条件(1)和(2)将被满足；当然，在这种情形，算子环的存在对群G的研究不能增加什么东西. 可是一般的情形很容易归结于这一情形和算子ε对应于恒等自同构的情形.

事实上，设已知一阿贝尔群G及其算子环R，R具有单位元ε. 我们用H表示G中那样一些元素a的集合，对于它们$a\varepsilon=a$；用F表G中使$a\varepsilon=0$的元素a的集合. H和F是群G的容许子群，它们的交只包含零元. H和F的直和等于群G，因为对于G中的任意元素a，等式

$$a=a\varepsilon+(a-a\varepsilon)$$

成立，其中显然有$a\varepsilon\in H$，$a-a\varepsilon\in F$. 在研究带算子的群时，我们

---

1) 等式左端的零是R中的零元，而右端的零则是群G中的零元.

当然有权只限于讨论直被加子群 H，对于 H 来说，ε 对应于它的恒等自同构. 今后，凡属讲到带单位元的算子环时，我们总假定这一限制已被满足，即假定条件

$$a\varepsilon=a \tag{3}$$

对 G 中所有元素 a 成立.

如果已知一带算子环 R 的群 G，则 R 中使群 G 里一个已知元素 a 零化的元素 α 所成集合，即使得 $a\alpha=0$ 的那些元素 α 的集合 $\mathfrak{a}$，将是环 R 中的一个右理想，这一点可由等式(1′)和(2)看出. 理想 $\mathfrak{a}$ 称为元素 a 的阶. 对普通的阿贝尔群，即以整数环 C 为算子环的群，这个定义实质上就是通常阶的定义：如果一个元素在普通意义下的阶是 n，则这个元素只能被 n 的倍数，即环 C 中由整数 n 所生成的理想中的元素所零化.

如果元素 a 的阶是环 R 中的零理想，则 a 称为无限阶元素. 例如，在无零因子环 R 中，如果将 R 本身看作它的加法群的右算子区，则除了零元之外，所有元素都是无限阶的. 群 G 中的零元的阶永远是整个环 R，并且如果所讨论的是带单位元的算子环的话，这还是唯一以 R 为阶的元素[参看条件(3)].

如果所讨论的算子环带有单位元的话，群 G 中由元素 a 所生成的(容许)循环子群(参看 §15)将由所有 $a\alpha$, $\alpha\in R$ 这种形状的元素所组成. 事实上，等式(1)表明这种元素在 G 内组成一个子群，由(2)可知这是一个容许子群，条件(3)表明元素 a 包含在这个子群内；最后，这个子群是循环群这一点，可由下面的事实看出，即任何一个容许子群如果包含元素 a 的话，必包含所有元素 $a\alpha$.

元素 a 的容许循环子群和商群 $\frac{R}{\mathfrak{a}}$ 带算子同构，其中 $\mathfrak{a}$ 是元素 a 的阶. 特别，如果 $\mathfrak{a}$ 是环 R 的双侧理想，则元素 a 的循环子环和剩余环 $\frac{R}{\mathfrak{a}}$ 的加法群带算子同构. 事实上，如果对 R 中的每个元素

α,使 G 中的元素 $a\alpha$ 和它相对应,那末根据(1)和(2)我们就得出一个带算子同态映射,将环 R 的加法群映成元素 a 的循环子群,并且被映成零元的元素恰是 $\mathfrak{a}$ 中的元素.

对阿贝尔群的一般理论中所得到的每一个结果,可以提出这样一个问题,即这个结果对带怎样一些算子环的群仍然保持正确.从这一观点来检查阿贝尔群理论整个内容的工作,虽然对环论本身也具有不容置疑的意义,可是现在还远没有完成.在这里,我们只指出和本章中前面几节里所证明的各个结果有关的几点事实:并且,为了避免过分繁琐起见,我们将假定算子环 R 是一个带单位元的无零因子环.

要使得群 G 的周期部分 F,即阶不等于零理想的元素的全体是 G 中的一个子群,只需假定环 R 中任意两个非零右理想的交不等于零即可,而这个子群的容许性则可由对环 R 附加交换性的假定得出.在这个情形,商群 $\frac{G}{F}$ 也将是一个 R-模,并且它里面所有不等于零元的元素都是无限阶的.

关于周期阿贝尔群可分解成准素群的直和的定理,需要对算子环 R 加上一些更强的限制才能得出.在任何情形下,要得出这个定理,只要假定 R 是的一个交换的主理想环就够了.

元素的线性相关性的定义,对带任意算子环的群仍然有意义.如果假定这个环是交换的,那末替换定理的证明也仍然有效.因而可以对群引入秩的概念.在这个假定下,关于一个群的秩等于它的任何一个(容许)子群的秩及对这个子群的商群的秩之和的定理,也仍然成立.

在具有算子环 R 的群的情形,环 R 本身的加法群,如果看作一个右 R-模的话,起着无限循环群的作用;相当于生成元的是环 R 的单位元或单位元的任何一个因子.任意一组这样的群的直和称

为一个自由 R-模. 如果 R 是一个交换环的话，自由 R-模的秩等于被加循环群的个数.

任何一个 R-模都与某一个自由 R-模的商群同构，并且，在 R 为交换环的情形，具 n 个生成元的 R-模和 n 秩自由 R-模的商群同构.

要证明这个定理，可将一个具有适当生成系的自由 R-模带算子同态地映到所讨论的 R-模上，并运用带算子群的同态定理.

如果环 R 中所有右理想都是主理想子环，则自由 R-模中任何一个不等于零的容许子群也是一个自由 R-模.

要证明这个定理，只需重复 §19 中相应定理的证明，并作如下的变动：如果考虑这个子群里具有给定末项足标 ν 的元素，那末在这个情形下不能说在这些元素当中存在具有最小正末项系数的元素. 可是很容易看出，所有这些元素的末项系数组成 R 中的右理想，根据我们的条件，这个理想将是一个主理想，即具有 $\{\alpha\}$ 这种形式. 这时，以 ν 为末项足标，以 α 为末项系数的元素，将起着具有最小正末项系数的元素的作用.

Everett[1]的工作中证明，这里对环 R 所加的条件——有单位元，无零因子，所有右理想都是主理想——也是使得自由 R-模的子群定理成立的必要条件.

要想把关于有限秩自由阿贝尔群的基与其子群的基之间的关系的定理，以及由这个定理所引出的关于具有限多生成元的阿贝尔群的基本定理推移到带算子阿贝尔群的情形，需要对算子环 R 加上一些更强的限制.在Teichmüller的论文[1]中证明，这些结果对环中所有右理想与左理想均为主理想的情形成立.对 R 为欧几里得环这个更特殊的情形，在Van der Waerden的《近世代数》第二版第十五章中有所讨论.[1] Teichmüller 的理论将在下一节叙述.

1) 或 Van der Waerden《代数学 II》§134（有中译本，科学出版社，1976）——译者注.

§ 22a Teichmüller 的理论

上面讲到，具有 n 个生成元的自由 R-模——这个模约定用 $U_n(R)$ 来表示——与它的容许子群 V 的基之间的关系的定理将在下面的假定下来证明：算子环 R 的所有左理想和所有右理想均为主理想．这就是说，如果 A 是环 R 的任意一个左（或右）理想，那末在 A 中可以找到这样一个元素 a，使得 $A=Ra$（或 $A=aR$）．首先引入一些新的概念，并且证明关于这种环的一系列结果．我们已经说过，所考虑的环都有单位元且没有零因子．

如果环 R 的元素 b 属于左理想 $Ra, a\neq 0$，即存在 R 的一个元素 r，使得 $b=ra$，那末元素 a 就叫做元素 b 的一个右因子．显然，在这一情形，$Rb\subseteq Ra$，如果 $Rb=Ra$，那么 b 同样也是元素 a 的一个右因子，即 $a=r'b$．因为 R 没有零因子，所以 $rr'=\varepsilon$，也就是说，r 和 r' 都是可逆元素．注意这时等式 $r'r=\varepsilon$ 也成立．事实上，由 $rr'=\varepsilon$ 推出 $r'rr'=r'$，又因为 R 没有零因子，所以 $r'r=\varepsilon$．元素 a 叫做 b 的一个左因子，如果 b 含在右理想 aR 内．元素 a 叫做元素 b 的一个全因子，如果它既是右因子，又是左因子，也就是说，如果 b 含在交 $Ra\cap aR$ 内．

设在环 R 里给定左理想 Ra 和 Rb，那末它们的和仍是一个主理想，即在 R 里可以找到这样一个元素 c，使得

$$(Ra, Rb)=Rc.$$

元素 c 叫做元素 a 与 b 的右最大公因子．因此，在 R 中存在元素 r', r'', r_1, r_2，使得

$$a=r'c, b=r''c, c=r_1a+r_2b.$$

类似地可以定义环 R 里两个元素的左最大公因子．

在环 R 里，不可能找到左理想的无限递增序列．

事实上，设在 R 里给定了左理想的一个无限不减序列

$$A_1\subseteq A_2\subseteq\cdots\subseteq A_n\subseteq\cdots.$$

这个序列的并集也是R的一个左理想，因而是由某一元素b所生成的主理想. 然而元素b含于某一理想A_n内，从而序列中从某一个开始，所有的理想都重合.

对于右理想来说，也有相应的定理.

在环R里不可能找到包含某一个非零左(右)理想A的无限递减左(右)理想序列.

考察任意的这样一个不增左理想序列

$$B_1\supseteq B_2\supseteq\cdots\supseteq B_n\supseteq\cdots$$

如果$A=Ra, a\neq 0, B_n=Rb_n, n=1,2\cdots$，那末存在这样的不等于零的元素$r_1, r_2,\cdots$和$r_1', r_2'\cdots$，使得

$$a=r_nb_n,\quad b_{n+1}=r_n'b_n, n=1,2,\cdots$$

于是

$$a=r_{n+1}b_{n+1}=(r_{n+1}r_n')b_n=r_nb_n,$$

即$r_{n+1}r_n'=r_n$. 这就表明，右理想

$$r_1R, r_2R,\cdots, r_nR,\cdots$$

构成一个不减序列. 根据上面所证明的事实，从某一个n开始，应该有等式

$$r_nR=r_{n+1}R=\cdots$$

然而由$r_nR=r_{n+1}R$得出，存在这样的元素r'，使得$r_{n+1}=r_nr'$，即$r_{n+1}=r_{n+1}(r_n'r')$，从而$r_n'r'=\varepsilon$. 因此，r_n'是一个可逆元素，从而$B_{n+1}=B_n$. 显然，对于一切$i>n$，都有$B_i=B_n$. 定理被证明.

R的一个非可逆元素a说是*既约的*，如果由等式$a=bc$必定可以得到或者b是可逆元素，或者c是可逆元素. 如果元素a可约，那末对于a的每一个被分成非可逆因子的乘积的分解$a=b_1b_2\cdots b_k$，就有一个左理想链

$$Ra\subset R(b_2\cdots b_k)\subset\cdots\subset Rb_k\subset R$$

与之对应，这些理想互不相同，并且都位于 Ra 与 R 之间．反之，如果在 Ra 与 R 之间给出了一个互不相同的左理想有限序列

$$Ra \subset Rc_1 \subset Rc_2 \subset \cdots \subset Rc_l \subset R$$

那末存在这样的非可逆元素 $b_1, b_2, \cdots b_l$，使得 $a=b_1c_1, c_1=b_2c_2, \cdots, c_{l-1}=b_lc_l$，从而

$$a=b_1b_2\cdots b_lc_l.$$

由上面所证明的关于理想链中断的定理推出(参看§16)，商群 R/Ra，作为以环 R 为(左)算子区的加群，具有合成列．对于这个群的每一个合成列，相应地就有元素 a 被分成有限多个不可约因子的乘积的一个分解．反之，由 Jordan-Hölder 定理推出，元素 a 的每一个这样的分解都有相同个数的因子．我们把这个数记作 $r(a)$．

如果 b 是元素 a 的一个左因子或右因子，那末元素 b 的每一个被分成不可约因子乘积的分解都可以补充成为元素 a 的一个这样的分解．因此 $r(b)\leqslant r(a)$．等号成立必要且只要 a 又是 b 的一个因子．对应于环 R 的元素 a 的正整数 $r(a)$ 的这个性质在下面将被用到．

现在转向带算子的阿贝尔群．

如果环 R 的一切右理想和一切左理想都是主理想，那末在自由模 $U_n(R)$ 和它的容许子群 V 里，可以分别选取这样的基 $\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_n$ 和 $\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_k, k\leqslant n$，使得

$$\bar{v}_i=\bar{u}_i\varepsilon_i, \quad i=1,2,\cdots,k,$$

这里每一个 ε_i 是 ε_{i+1} 的一个全因子．

证明可按§20中相应定理的证明的同样程式来进行．因此，我们把证明的细节留给读者去做，而只限于指出由以整数环作为算子区的情形过渡到现在所考虑的情形的不同之处．

注意到这时容许子群是环 R 的右理想，因而是主理想，所以定

理对于 $n=1$ 正确.

在 § 20 所给的证明里，组成子群 V 的那些线性到式里的最小正系数扮演着重要角色. 这个角色现在要由这样一个不等于零的系数 α 来充当，对于这个 α 来说，$r(\alpha)$是最小的.

再者，现在不能施行带余除法. 在我们的证明里，将由以下两个引理来代替.

引理 1 如果在模 $U_n(R)$ 的元素

$$u=u_1\alpha_1+u_2\alpha_2+\cdots+u_n\alpha_n$$

里，系数 α_1 和 α_2 都不等于零，而 δ 是元素 α_1 与 α_2 在环 R 内的一个右最大公因子，那末可以变更模 $U_n(R)$ 的基，使得在元素 u 关于新基的表示式里，δ 作为一个系数出现.

根据题设，$(R\alpha_1, R\alpha_2)=R\delta$. 于是在 R 里存在元素 α_1'，α_2'，ξ 和 η，使得

$$\alpha_1=\alpha_1'\delta, \alpha_2=\alpha_2'\delta, \tag{1}$$

$$\xi\alpha_1+\eta\alpha_2=\delta.$$

由此得

$$\xi\alpha_1'+\eta\alpha_2'=1. \tag{2}$$

由(2)可以得出等式

$$\alpha_1'\eta\alpha_2'=\alpha_1'-\alpha_1'\xi\alpha_1', \tag{3}$$

$$-\alpha_2'\xi\alpha_1'=\alpha_2'\eta\alpha_2'-\alpha_2'. \tag{4}$$

这两个等式都有一边属于理想 $R\alpha_1'$，另一边属于理想 $R\alpha_2'$，因此两边都属于这两个理想的交. 这个交仍是环 R 的一个左理想，并且由一个非零元素生成，因为等式(3)和(4)的左边至少有一个不等于零. 因此，存在一个元素 β，$\beta\neq 0$，使得

$$R\alpha_1'\cap R\alpha_2'=R\beta.$$

由此推出，存在这样的元素 σ，τ，μ 和 ν，使得

$$\beta=\sigma\alpha_1'=-\tau\alpha_2', \tag{5}$$

$$\mu\beta=\alpha_1'\eta\alpha_2'=\alpha_1'-\alpha_1'\xi\alpha_1', \tag{6}$$

$$\nu\beta=-\alpha_2'\xi\alpha_1'=\alpha_2'\eta\alpha_2'-\alpha_2'. \tag{7}$$

现在令

$$u_1'=u_1\alpha_1'+u_2\alpha_2',$$
$$u_2'=u_1\mu+u_2\nu,$$
$$u_i'=u_i,\ i=3,\cdots,n.$$

则它们构成模$U_n(R)$的一个基．事实上，由变换

$$u_1=u_1'\xi+u_2'\sigma,$$
$$u_2=u_i'\eta+u_2'\tau,$$
$$u_i=u_i',\ i=3,\cdots,n,$$

就可以返回到原来的基，这一点利用等式(2)，(5)，(6)，(7)，并且注意到环R没有零因子，就可以验证．根据(1)和(5)，我们现在就得到

$$u=u_1'\delta+u_3'\alpha_3+\cdots+u_n'\alpha_n.$$

引理被证明．

引理2　如果模$U_n(R)$的子模V含有元素

$$v_1=u_1\alpha_1+u_2\alpha_2+\cdots+u_n\alpha_n,$$
$$v_2=u_1\beta_1+u_2\beta_2+\cdots+u_n\beta_n,$$

其中系数α_1和β_1都不等于零，而δ是元素α_1与β_1在环R内一个左最大公因子，那末δ将在子模V的某一元素的表示式里作为u_1的系数出现．

事实上，由$(\alpha_1R,\alpha_2R)=\delta R$推出，在$R$里存在元素$\xi$和$\eta$，使得$\alpha_1\xi+\beta_1\eta=\delta$．于是在子模$V$里，含有元素

$$v=v_1\xi+v_2\eta=u_1\delta+\cdots.$$

引理被证明．

最后，注意到若是在$U_n(R)$和在V里，各选出基$\bar{u}_1,\bar{u}_2,\cdots,\bar{u}_n$和$\bar{v}_1,\bar{v}_2,\cdots,\bar{v}_k$，使得

$$\bar{v}_i = \bar{u}_i \varepsilon_i, \ i = 1, 2, \cdots, k,$$

那末按以下的办法来证明 ε_1 是 ε_2 的全因子.

在子模 V 里含有元素

$$\bar{v}_1 + \bar{v}_2 = \bar{u}_1 \varepsilon_1 + \bar{u}_2 \varepsilon_2.$$

根据元素 ε_1 的选取和引理 1, 元素 ε_1 是 ε_2 的右因子. 另一方面, 如果在模 $U_n(R)$ 内选取基 $\bar{u}_1, \bar{u}_2 - \bar{u}_1, \bar{u}_3, \cdots, \bar{u}_n$, 那末

$$\bar{v}_1 = \bar{u}_1 \varepsilon_1, \bar{v}_2 = \bar{u}_1 \varepsilon_2 + (\bar{u}_2 - \bar{u}_1) \varepsilon_2.$$

由此, 再根据元素 ε_1 的选取和引理 2 可知, ε_1 是 ε_2 的左因子.

如同不带算子群的情形一样, 由现在所证明的定理可以证明, 在每一个右理想和每一个左理想都是主理想的算子环上, 任意一个具有限个生成元的模都可以分解成有限个容许循环子群的直和. 如果再假定算子环是交换环, 那末还可以将其中生成元的阶不为零的那些循环被加项再进一步分解成这样的循环子群的直和, 这些循环子群的阶是由运算子环的素元素(即既约的元素)的幂生成的. 这个断语的证明实质上接近 §20 中对应定理的证明, 但不要求主理想交换环理论的某些补充知识, 因此从略.

第七章　准素阿贝尔群与混合阿贝尔群

§23.　完备阿贝尔群

准素阿贝尔群的理论是阿贝尔群的一般理论中内容最丰富和最深入的几个分支之一，其中可数准素群的理论可以说已经完成．准素群理论中的许多部分——完备群的理论，纯子群的问题及其他问题——现在已经超出了准素群的范围．因此，最好将准素群的理论密切结合着混合群的理论来讲述；并且，在这一途径上还可以找到一个最自然的方法来处理混合群理论中的一个基本问题——混合群的分解问题，亦即将混合群分解成为周期群与无扭群的直和的问题．

我们先从一类非常重要的阿贝尔群的研究开始．这一类群在某种意义上是和自由阿贝尔群相对立的．

阿贝尔群 G 称为一个*完备群*，如果对 G 中任意元素 a 和任意自然数 n，方程

$$nx=a$$

在 G 中至少有一个解，即如通常所说的，元素 a 在群 G 里可被任意一个自然数*除尽*．显然，要使阿贝尔群 G 是一个完备群，只要它的任何一个元素都能被任意素数除尽就行了．

从定义直接可以推出，*完备群的任意一个商群也是完备群*，此外，*任意一组完备群的直和是完备群*．

如果阿贝尔群 G 包含一个完备子群 A，则 A 可作为一个直被加群从 G 中分解出来．

事实上，设 B 是群 G 中和 A 的交等于零的极大子群里的一个，这样的子群的存在可由 §7 中所证明的定理推出．子群 A 和 B 构成群 G 中的一个直和．如果在群 G 中可以找到一个不属于 $A+B$

的元素 g，则子群 $A+B$ 和 $\{g\}$ 的交不可能等于零，因为不然的话，子群 A 和 $B+\{g\}$ 的交也会等于零，而这是和 B 的选择相矛盾的. 因此，元素 g 必有一个倍元包含在 $A+B$ 内，即

$$pg=a+b,\ a\in A,\ b\in B;$$

这里 p 可以看作是一个素数——只要将 g 换成它的这样一个倍元，使这个倍元本身不包含在 $A+B$ 内，但它的一个素倍元包含在 $A+B$ 内就行了.

在 A 内可以找到一个元素 a'，使 $pa'=a$. 于是就有

$$p(g-a')=b\in B,\ g-a'\in A+B.$$

引用记号 $g'=g-a'$. 子群 $\{g',B\}$ 中的任何一个元素都有 $kg'+b'$ 这种形状，其中 $0\leqslant k\leqslant p-1$, $b'\in B$. 如果子群 A 和 $\{g',B\}$ 的交不等于零，则在 A 里可以找到一个元素 $\bar{a}$, $\bar{a}\neq 0$，使

$$\bar{a}=k'g'+b',$$

这里 $k'\neq 0$，因为 $A\cap B=0$. 但因 $pg'\in B$ 而整数 p 与 k' 互素，故从这个等式不难得出 $g\in A+B$，而这是不可能的. 在另一方面，如果子群 A 和 $\{g',B\}$ 的交等于零，又与子群 B 的选择相矛盾. 这就证明了 $G=A+B$.

一个阿贝尔群中任意一组完备子群的和是完备子群.

事实上，如果已知阿贝尔群 G 中的一组完备子群 A_α，则这些子群的和中的任何一个元素具有

$$a_{\alpha 1}+a_{\alpha 2}+\cdots+a_{\alpha k}$$

这种形状，其中 $a_{\alpha i}\in A_{\alpha i}$. 如果 $p\bar{a}_{\alpha i}=a_{\alpha i}$, $i=1,2,\cdots,k$，则元素 $\bar{a}_{\alpha 1}+\bar{a}_{\alpha 2}+\cdots+\bar{a}_{\alpha k}$ 包含在子群 A_α 的和内，且

$$p(\bar{a}_{\alpha 1}+\bar{a}_{\alpha 2}+\cdots+\bar{a}_{\alpha k})=a_{\alpha 1}+a_{\alpha 2}+\cdots+a_{\alpha k}.$$

特别，阿贝尔群 G 中所有完备子群的和 $\bar{A}$ 是 G 中的极大完备子群. 在直分解

$$G=\bar{A}+G'$$

(根据上面所证的定理这种分解是存在的)中，子群G'不再包含完备子群. 如果我们把一个不包含任何完备子群的阿贝尔群称为既约的，则任何一个阿贝尔群可分解成为两个群——一个既约群和一个完备群的直和. 阿贝尔群G可能有许多种这样的直分解，但是在所有这种分解中的完备部分永远是相同的，因而既约部分彼此同构.

不难将所有完备阿贝尔群全部描述出来. 完备阿贝尔群当中显然包括R型群，即和全体有理数的加法群同构的群，以及对所有素数p的p^{∞}型群(参看§7). 事实上，由p^{∞}型群的定义可知它里面的任何一个元素可被p除尽；至于用任何一个不等于p的素数来除这个元素，则这一点在由这个元素所生成的p^n阶循环群里就已经可以作到了. 研究的结果证明，上面所讲的这两类群及其直和就是全部的全备群.

任何一个完备阿贝尔群可分解成一组R型群和对某些素数p的p^{∞}型群的直和.

事实上，完备阿贝尔群G的周期部分F也是一个完备群，因为如果a是有限阶的，则方程$nx=a$的任意一个解x也是有限阶的. 由此，如上面所证，可知存在直和分解

$$G=F+H,$$

其中H是一个无扭群，并且因为它和一个完备群的商群同构，所以也是完备的. 另一方面，在§19中已经证明子群F可分解成为对不同素数p的准素群F_p的直和. 这里每一个子群F_p都是完备的：如果$a\in F_p$，则方程$px=a$的解以p的一个幂为阶，因而包含在F_p内，而任何一个方程$qx=a$，如果$(q,p)=1$的话，则如我们所知道的，在子群$\{a\}$里就可解.

因此，只要讨论两种特殊情形——无扭完备群的情形和对p的准素完备群的情形就行了.

如果 G 是一个无扭完备群，a 是它的一个不等于零的元素，则适合条件

$$a_1=a, na_n=a_{n-1}, n=2,3,\cdots$$

的元素 $a_1, a_2, \cdots, a_n, \cdots$（由群 G 的完备性可知这样的元素存在）在 G 里生成一个 R 型子群（参看 § 18 例 2）. 设 M 是群 G 的一个极大线性无关元素系. 我们用上面所指出的方法将 M 中的每一个元素嵌入一个 R 型子群内. 由元素系 M 的线性无关性可知，这些子群的和 G' 将是直和. 此外，这个和等于整个群 G. 事实上，G 中任何一个元素 b 都和 M 线性相关，也就是说，存在一个等式

$$nb=k_1a_1+k_2a_2+\cdots+k_sa_s,$$

其中 $n\neq 0$, $a_1, a_2, \cdots, a_s\in M$. 然而从完备群 G' 里可以找到一个元素 c，使 c 和 M 以同一线性关系式相关联. 由此即有 $n(b-c)=0$，因而 $b=c, G'=G$.

讨论对素数 p 的准素群的情形时，首先注意，准素完备群中的任何一个元素都包含在一个 p^∞ 型子群内. 事实上，如果已知完备群中的一个 p^k 阶元素 a，那末我们可引入记号

$$a_1=p^{k-1}a, a_2=p^{k-2}a, \cdots, a_{k-1}=pa, a_k=a,$$

然后从 p 倍等于 a_k 的元素当中选出一个作为 a_{k+1}. 一般地如果元素 a_n, $n\geqslant k$ 已经选定，那末可以选方程 $px=a_n$ 的一个解作为元素 a_{n+1}. 元素 $a_1, a_2, \cdots, a_n, \cdots$ 显然生成一个包含元素 a 的 p^∞ 型子群.

利用这一点，可以在准素完备群 G 中用一个通常的超穷过程选出一组 p^∞ 型子群，使它们的和 G' 是直和，并使得在 G 里不能再选出另外的 p^∞ 型子群来，使它和 G' 的交等于零. 我们证明 G' 与 G 重合. 事实上，如果 G 包含一个不属于 G' 的元素 a，并且子群 G' 与 $\{a\}$ 的交等于零，则将 a 嵌入一个 p^∞ 型子群之后，我们将会得出一个和子群 G' 的定义相矛盾的结果. 如果 $p^ka\in G'$，但 $p^{k-1}a\notin$

G'，则由于子群 G' 的完备性，从它里面可以找到一个元素 a'，使 $p^k a' = p^k a$；元素 $a - a'$ 不等于零，但它所生成的循环子群和 G' 的交等于零．这个情形正是我们所已经讨论过的．这样就证明了群 G 是一些 p^∞ 型群的直和．

定理证毕．

特别，由这个定理可知，所有实数的加法群是一个具有连续统势的无扭完备群，因而可以分解成为一批 R 型群的直和，这批 R 型群所成的集合具有连续统势．

完备阿贝尔群的任何一个直分解，可以继续分解到 R 型群与 p^∞ 型群的直和．将完备阿贝尔群分解成 R 型群与 p^∞ 型群的任意两个直分解彼此同构．

这定理的第一个命题可由下面的事实得出，即完备群的任何一个直被加群也是完备群——如果 $G = A + B$，$n(a' + b') = a$ 其中 $a', a \in A, b' \in B$，则 $na' = a$，——因而如以上所证，可分解成为一些 R 型群和 p^∞ 型群的直和．

为了证明第二个命题，我们取任意一个将群 G 分解成 R 型群与 p^∞ 型群的直分解加以考虑．从这个分解中的每一个 R 型直被加群中各取出一个不等于零的元素，我们就得出群 G 中的一个极大线性无关元素系；因此，由 § 19 中的结果可知，R 型被加群的个数（这种被加群的集合的势）和直分解的选择无关．另一方面，固定素数 p 并作这个分解中所有 p^∞ 型被加群的直和，我们就得出群 G 的一个子群 A，这个子群由 G 中阶是有限的且等于 p 的幂的全体元素所组成，因而和直分解的选择无关．如果这个直分解中的 p^∞ 型被加群的个数是 n，则子群 A 中阶不大于 p 的元素的个数等于 p^n；如果子群 A 中这种元素有无限多个，则这些元素的集合的势等于群 G 的这一直分解中 p^∞ 型被加群的集合的势．这就证明了 p^∞ 型被加群的个数（这些被加群的集合的势）也和直分解的选

择无关. [参看补充. 28.5.]

任何一个无扭完备阿贝尔群G都是有理数域$\mathfrak{R}$上的向量空间.

事实上,如果a和b是群G的元素而$ma=nb$, 那么给定数m和n以及元素a,b 中的一个,另一个也就唯一地被确定. 如果$n\neq0$,那末可以使用写法$b=\frac{m}{n}a$,并且把元素b看成对元素a作用有理数域$\mathfrak{R}$中的算子$\frac{m}{n}$的结果. 事实上,容易验证,有单位元的环上模的定义里(参看§22)条件成立.

现在容易看出,无扭完备阿贝尔群的包含元素a的R型子群由所有形式如$\frac{m}{n}a$的元素所组成, 以下我们约定把这个子群写作$\mathfrak{R}a$. 因此,如果G是一个有限秩的无扭完备群而$a_1, a_2, \cdots, a_n$是它的一个极大线性无关系,那么如以上所证,

$$G=\mathfrak{R}a_1+\mathfrak{R}a_2+\cdots+\mathfrak{R}a_n.$$

我们同时还约定,如果A是无扭完备群G的一个子集, 而$\mathfrak{R}'$是域$\mathfrak{R}$的一个子环,就用$\mathfrak{R}'A$表示群G中包含A并且容许$\mathfrak{R}'$中算子作用的最小子群. 这样, 若M是群G的一个极大线性无关系, 那么$\mathfrak{R}M=G$. 特别地,这个记法我们将在§§ 32б, 32в 中使用.

回到一般情形,我们证明以下重要的定理.

任何一个阿贝尔群都是某一完备阿贝尔群的子群

这个定理的下述简单证明是 Куликов[2]给出的. 我们已经知道,阿贝尔群G可以表成一个自由阿贝尔群U的商群的形式:

$$G=\frac{U}{N}.$$

任意取一个将群U分解成无限循环群的直分解. 将每一个被加循环群嵌入一个R型群——譬如说, 用普通将整数加法群嵌入

有理数加法群的方法——，并作所有这些 R 型群的直和，我们就得出一个包含 U 的完备群 V，商群 $\frac{V}{N}$ 也是一个完备群，并且包含 $\frac{U}{N}$，即包含 G.

前面我们已经证明，完备群可作为一个直被加群从任何一个包含它的阿贝尔群中分解出来. 从上面的定理可推出这个定理的一个逆定理(参看 Baer[26])：

如果阿贝尔群 G 可以从任何一个包含它作为子群的阿贝尔群中作为一个直被加群分解出来，则这个群必是完备群.

事实上，群 G 特别应该作为任何一个包含它的完备群的一个直被加群. 可是我们知道完备群的任何一个直被加子群也是完备群.

下面的定理部分地包括在 Baer 的论文[26]内，完全的证明则是 Куликов 给出的，这个定理补充了关于任何一个阿贝尔群可嵌入完备群内的定理.

在任何一个包含已知群 G 的完备阿贝尔群里，至少可以找出一个完备子群来，使它在所有包含 G 的完备子群中为极小. 在任何两个包含 G 的极小完备群之间必有一个同构对应，使它是群 G 的恒等自同构的延拓.

事实上，设群 G 包含在完备群 $\bar{G}$ 内. 因为一个递增完备群列的并集还是一个完备群，故群 $\bar{G}$ 中与 G 的交等于零的完备子群当中存在极大的. 设 H 是这种完备子群之一. 存在一个直分解

$$\bar{G}=H+F,$$

并且，如我们所知道的，可以选择子群 F，使包含子群 G. 作为一个完备群的直被加子群 F 也是完备的，并且这就是我们所要求的包含 G 的极小完备子群. 事实上，如果存在一个包含于 G 和 F 之间的完备子群 F'：

$$G \subset F' \subset F,$$

则

$$F = F' + F'',$$

即

$$\bar{G} = F' + (F'' + H).$$

子群 F'' 是完备的，因而 $F'' + H$ 也是完备的，但因子群 $F'' + H$ 与 G 的交等于零，故我们得出了和子群 H 的选择相矛盾的结果.

现在设 F_1 和 F_2 是包含群 G 的任意两个极小完备子群. 由于群 G 的不完备性，在它里面可以找到一个元素 a，使对某一素数 p，方程

$$px = a$$

在 G 中没有解. 设 b_1 和 b_2 分别是这个方程在 F_1 和 F_2 中的解. 如果将子群 G 恒等地映成其自身，并命 $b_1\varphi' = b_2$，我们就得出子群 $F_1' = \{G, b_1\}$ 和 $F_2' = \{G, b_2\}$ 之间的一个同构对应 φ'.

设对小于某一 α 的所有序数 β 都已在 F_1 中找到了构成一个递增列的子群 $F_1^{(\beta)}$，在 F_2 中找到了子群 $F_2^{(\beta)}$，并且在子群 $F_1^{(\beta)}$ 和 $F_2^{(\beta)}$ 之间建立了同构对应，使每个同构对应都是前面的同构对应的延拓. 如果 α 是一个极限序数，我们就用 $F_i^{(\alpha)}$ $(i=1,2)$ 表示子群 $F_i^{(\beta)}$ 的并集，并将同构 $\varphi^{(\beta)}$ $(\beta<\alpha)$ 的并集当作 $\varphi^{(\alpha)}$. 如果 $\alpha-1$ 存在，则可设 a_1 为 $F_1^{(\alpha-1)}$ 中的这样一个元素，使对某一素数 p，方程

$$px = a_1,$$

在 $F_1^{(\alpha-1)}$ 中没有解，并用 b_1 表示这个方程在 F_1 中的解. 如果 $a_1\varphi^{(\alpha-1)} = a_2$，而 b_2 是方程

$$px = a_2$$

在 F_2 内的解，我们就命

$$F_i^{(\alpha)} = \{F_i^{(\alpha-1)}, b_i\}\ i = 1, 2.$$

在 $F_i^{(\alpha-1)}$ 上和 $\varphi^{(\alpha-1)}$ 重合而将 b_1 映成 b_2 的映射 $\varphi^{(\alpha)}$ 将是 $F_1^{(\alpha)}$ 和 $F_2^{(\alpha)}$ 之间的一个同构.

这个构造方法可以一直继续下去，直到子群 $F_1^{(\alpha)}$ 和 $F_2^{(\alpha)}$ 是完备群时，即直到它们分别与 F_1 及 F_2 重合时为止. 定理证毕.

注意，一个完备群里的确可能存在多个包含已知子群 G 的极小完备子群. 例如，设 A 和 B 是两个 p^∞ 型群，A 的生成元是

$$a_1, a_2\cdots, a_n, \cdots,$$

定义关系是

$$pa_1=0, pa_{n+1}=a_n, n=1, 2\cdots,$$

B 的生成元是

$$b_1, b_2, \cdots, b_n, \cdots$$

定义关系是

$$pb_1=0, pb_{n+1}=b_n, n=1, 2, \cdots,$$

则在它们直和中，子群 $\{a_1\}$ 包含在子群 A 内，也包含在由元素

$$a_1, a_2+b_1, \cdots, a_n+b_{n-1}, \cdots$$

所生成的 p^∞ 型子群内. [参看补充. 28. 4.]

§24. 循环群的直和

我们已经研究过了可以分解成循环群直和的两类阿贝尔群，即：自由阿贝尔群——也就是任意多个无限循环群的直和，和具有限多个生成元的阿贝尔群——也就是有限多个任意循环群的直和. 这些群有一系列的共同性质，我们要证明这些性质是任意多个任意循环群的直和所具有的性质. 显然，在研究这些群的时候，可以假定这些直和中所有有限被加循环群都是对某些素数的准素群.

关于阿贝尔群能否分解成循环群的直和的问题，有许多判定法. 现在我们就要举出这些判定法中的一个，这是关于准素群情

形的判定法. 但是我们先要引进一些概念，这些概念对整个准素阿贝尔群的理论都是基本的.

如果群 G 是(对某一素数 p 的)一个准素群，则它里面所有 p 阶元素(包括零元在内)的集合是一个子群，这个子群甚至还是一个全特征子群，称为群 G 的*底层*.

准素群 G 的元素 a 称为一个*无限高度元素*，如果 $a\neq 0$，而对任意 k，方程

$$p^k x = a$$

在群 G 中至少有一个解. 如果这个方程只有在 $k\leqslant n$ 时才在 G 里可解，那我们就说元素 a 具有*有限高度*，即*高度 n*.

应该指出，确切一点的说法应是*元素 a 在群 G 中的高度*，因为这个元素在群 G 的子群 H 里的高度可能比它在整个群 G 中的高度来得小.

由高度的定义立即可得出元素的高度具有下述性质. 如果元素 a_1 和 a_2 在群 G 中分别有高度 h_1 和 h_2，则在 $h_1<h_2$ 时元素 a_1+ $+a_2$ 的高度等于 h_1，而在 $h_1=h_2=h$ 时则这个和的高度大于或等于 h. 如果元素 a 的高度是 h，则元素 pa 的高度大于或等于 $h+1$. 如果元素 a 和 b 生成同一循环子群；则它们在群 G 中的高度相等. 如果群 G 可分解成直和，那末包含在某一被加子群里的元素在该子群中的高度等于它在整个群 G 中的高度. 一个直和中任意元素的高度，等于在它的各个分支中所有高度里面最小的一个.

在完备准素群中，并且只有在这种群中，所有元素都有无限高度. 除此之外，*如果准素群 G 的底层中每一个元素都在 G 中有无限高度，则 G 是完备群.* 事实上，设已经证明群 G 中所有 p^n 阶元素都有无限高度. 如果 a 是这些元素里面的任意一个，b_1 和 b_2 是方程 $px=a$ 的任意两个解，则元素 b_1-b_2 是一个 p 阶元素，因而具有无限高度. 由此根据上段中的第一命题，元素 b_1 和 b_2 有相同

高度．但因元素 a 有无限高度，故在方程 $px=a$ 的解中可以找到高度大于任何预定自然数的元素．因此，对任意 p^n 阶元素 a，方程 $px=a$ 的所有解——即所有 p^{n+1} 阶元素在 G 里有无限高度．

现在我们证明 Куликов[2]的下述判定法．

准素阿贝尔群 G 可分解成循环群的直和的充分必要条件，是它能够表成这样一个递增子群列：

$$A^{(1)}\subseteq A^{(2)}\subseteq\cdots\subseteq A^{(n)}\subseteq\cdots \qquad (1)$$

的并集，其中每一个子群里的元素在群 G 中的高度都是有限的，而且全体有界．

证明．如果群 G 已经表成了一些循环群的直和，则可取这一分解中阶不大于 p^n 的循环被加子群的和作为子群 $A^{(n)}$，$n=1, 2,\cdots$．

反之，设群 G 可表成满足所述条件的递增群列(1)的并集．我们从子群 $A^{(1)}$ 的 p 阶元素当中取出一个在 G 中具有最大可能高度的元素作为 x_1；这样的元素是存在的，因为子群 $A^{(1)}$ 中的元素在群 G 中的高度全体有界．

兹假设对小于某序数 β 的所有序数 α，在群 G 中都已选出了适合下列条件的元素 x_α；

1) 所有元素 x_α 的阶都是 p；

2) 如果元素 x_α 包含在子群 $A^{(n)}$ 内，但不包含在 $A^{(n-1)}$ 内，且 C_α 是由所有元素 x'_α $(\alpha'<\alpha)$ 所生成的子群，则：

a) 子群 C_α 包含子群 $A^{(n-1)}$ 的整个底层 $A_1^{(n-1)}$；

б) x_α 不包含在子群 C_α 内，且子群 $A^{(n)}$ 的不属于 C_α 的所有元素当中以 x_α 在群 G 中的高度为最大．

如果由所有元素 $x_\alpha(\alpha<\beta)$ 所生成的子群 C_β 还不等于整个群 G 的底层 G_1，那末还可以用下面的方法选出一个元素 x_β：由2a)可知，在这样的情况下必存在一个自然数 n，使所有元素 x_α 都包含在

$A^{(n)}$内，但不全都包含在$A^{(n-1)}$内．如果子群C_β不等于$A_1^{(n)}$，那末我们可从子群$A^{(n)}$中不属于C_β的p阶元素当中选出一个在G中具有最大高度的元素作为x_β．如果C_β和$A_1^{(n)}$重合，那末我们就从序列(1)中底层大于C_β的最小子群中选出一个类似的元素作为x_β．显然，在两种情况下我们都利用到了定理表述中对子群$A^{(n)}$所加上的要求．

因此，选择元素x_α的过程可以一直继续下去，直到这些元素能够生成群G的整个底层为止．设在对小于γ的所有α选出元素x_α时，元素x_α生成群G的整个底层．由1)和2б)可知，群G的底层有一个直分解

$$G_1=\sum_{\alpha<\gamma}\{x_\alpha\}. \tag{2}$$

设元素x_α在群G中的高度是h_α，而y_α是G中的这样一个元素，使

$$p^{h_\alpha}y_\alpha=x_\alpha.$$

由于(2)，循环群$\{y_\alpha\}$构成一个直和，这个直和我们用F来表示

$$F=\sum_{\alpha<\gamma}\{y_\alpha\}. \tag{3}$$

兹证明群G中的任何一个p阶元素z（由于$G_1\subset F$，元素z必包含在F内）在子群F内的高度和它在整个群G中的高度相等。事实上，根据(2)，元素z可写成

$$z=x'_{\alpha_1}+x'_{\alpha_2}+\cdots+x'_{\alpha_n}$$

这种形状，其中$x'_{\alpha_i}(i=1,2,\cdots,n)$是元素$x_{\alpha_i}$的非零倍元，因而在群$G$中和子群$F$中有同一高度$h_{\alpha_i}$．由于直分解(3)，元素$z$在子群$F$中的高度$h$等于整数$h_{\alpha_i}(i=1,2,\cdots,n)$中最小的一个．这个元素在群$G$中高度不可能比$h$小；现在我们证明这两个高度也不可能比$h$大．设$k$是这样一个足数，使得$h_{\alpha_k}=h$，但在$i>k$时$h_{\alpha_i}>h$．这时和

$$z=(x'_{\alpha_1}+\cdots+x'_{\alpha_k})+(x'_{\alpha_{k+1}}+\cdots+x'_{\alpha_n})$$

中的第二项或者不存在(当 $k=n$ 时)，或者它在群 G 中的高度严格大于 h. 至于第一项，则因为它不包含在子群 C_{α_k} 内，故它在 G 中的高度不能大于元素 x_{α_k} 在 G 中的高度，也就是说，不能大于 $h_{\alpha_k}=h$，因为不然的话，我们就会得出与对元素 x_{α_k} 的选择所附加的条件 2б）相矛盾的结果. 由此可知，元素 z 是 G 中高度不同的两个元素的和，它在群 G 的高度等于这两个高度中的较小者，因而不会比 h 大. 这就证明了元素 z 在 G 和 F 中有同一高度.

现在假定 G 不等于 F. 设 g 是群 G 中不属于 F 的元素中阶最小的一个，并设其阶为 p^s；显然 $s\geqslant 2$. 元素 $p^{s-1}g$ 的阶等于 p，因而包含在 F 内，并且，如以上所证，在 F 和 G 中有同一高度. 因此，在 F 中可以找到一个元素 f，使

$$p^{s-1}f=p^{s-1}g.$$

元素 $g-f$ 的阶不大于 p^{s-1}，也就是说，元素 $g-f$ 包含在 F 内，但这样一来，元素 g 也应属于 F，而这和我们的假定相反. 这就证明了等式 $G=F$. 判定法的证明到此结束. [参看补充. 28.2.]

由这个判定法可以推出Prüfer[2]的下叙两个定理，在准素阿贝尔群的理论中，这是两个基本定理.

Prüfer第一定理： 元素的阶全体有界的准素阿贝尔群可分解成循环群的直和.

事实上，在这一情形下所有元素的高度都是有限的，并且全体有界. 因此可以命所有子群 $A^{(n)}$ 等于整个群，而应用 Куликов判定法.

Prüfer第二定理： 不包含无限高度元素的可数准素群，可分解成循环群的直和.

事实上，由于它的可数性. 这个群可以表成它的具有限多个生成元的子群的递增列的并集，并且由群的周期性与交换性可知，

这些子群全是有限群. 根据我们的条件，每个子群中的元素在整个群中的高度都是有限的，但因为这些元素只有有限多个，故元素的高度全体有界.

由 Куликов 判定法还可以引出下述结果的一个简单证明.

可分解成循环群的直和的准素群 G 中，每一个子群 H 也可以分解成循环群的直和.

事实上，根据 Куликов 判定法，群 G 可表成一个递增子群列 $A^{(n)}(n=1,2,\cdots)$ 的并集，其中每个子群 $A^{(n)}$ 中所有元素在群 G 中的高度都是有限的，且全体有界. 如果

$$B^{(n)}=H\cap A^{(n)},\quad (n=1,2,\cdots),$$

则每个子群 $B^{(n)}$ 中所有元素在群 G 中高度都是有限的，且全体有界，其在子群 H 中的高度当然更是如此. 但子群 H 是子群 $B^{(n)}$ 的并集，故只要再用一次 Куликов 判定法就行了.

现在我们可以停止对准素群的讨论，重新回到一般的情形上来. 由前面的结果和 § 19 中的关于自由阿贝尔群的子群的定理，可以得出下面的一个一般结果.

可分解成循环群的直和的阿贝尔群 G 中，每一个子群 H 也可以分解成循环群的直和.

事实上，如果 G^* 是群 G 的周期部分，则因群 G 是循环群的直和，它就可以分解成子群 G^* 和一个自由子群 S 的直和. 根据同构定理，子群 H 对其周期部分 H^* 的商群与群 $\frac{G}{G^*}$ 的一个子群同构，也就是说，与群 S 的一个子群同构. 因此，群 $\frac{H}{H^*}$ 是一个自由群的子群，因而也是一个自由群. 这就是说，群 H 可表成子群 H^* 和一个自由子群的直和(见 § 19 末尾处). 其次，群 G^* 是对不同素数 p 的准素子群的直和，且每一个这样的子群都是循环群的直和. 子群 H^* 可分解成为它和这些准素群之交的直和. 最后只要利用上面

所证明的关于可分解成循环群直和的准素群的子群定理就行了.

如果阿贝尔群 G 可分解成循环群的直和，则这个群的任何一个直分解可以继续分解到成为循环群的直和.

事实上，根据上面的定理，群 G 的每个直被加子群可以分解成循环群的直和.

如果阿贝尔群 G 可分解成循环群的直和，则任意两个将 G 分解成无限循环群和有限准素循环群的直分解彼此同构.

事实上，在这两个直分解中被加的无限循环群的个数等于群 G 的秩，因而与直分解的选择无关. 其次，一个直分解中，阶为素数 p 的幂的那种被加群，生成一个和直分解的选择无关的准素子群. 因此只要考虑群 G 本身为准素群的情形就行了.

任取一个将群 G 分解成循环群的直分解，并用 $A^{(n)}$ 表示这个直分解中阶为 p^n 的直被加群的和；如果这样的直被加群不存在，则命 $A^{(n)}=0$. 于是我们有

$$G=A^{(1)}+A^{(2)}+\cdots+A^{(n)}+\cdots,$$

与此相应，群 G 的底层分解成群 $A^{(n)}$ 的底层的直和

$$G_1=A_1^{(1)}+A_1^{(2)}+\cdots+A_1^{(n)}+\cdots,$$

设

$$B^{(n)}=A_1^{(n)}+A_1^{(n+1)}+\cdots,$$

则

$$B^{(n)}=A_1^{(n)}+B^{(n+1)},$$

由此即有

$$A_1^{(n)}\simeq B^{(n)}/B^{(n+1)},\quad n=1,2,\cdots$$

然而很容易看出，子群 $B^{(n)}(n=1,2,\cdots)$ 可以不依赖于所讨论的群 G 的直分解而确定：这个子群包含群 G 中高度不小于 $n-1$ 的所有 p 阶元素，并且仅包含这样一些元素. 因此，子群 $A_1^{(n)}$ 除一同构之差外，可由群 G 本身所决定；但因为群 $A^{(n)}$ 作为阶数同为 p^n 的循

环群的直和，可由它的底层及数 n 所完全决定，于是任意两个将群 G 分解成循环群的直分解之间的同构关系就此证明.

最后，从循环群直和的子群定理可以证明下面的命题.

任何一个阿贝尔群都是一个由循环群直和所构成的可数递增列的并集.

对于完备群来说，这是很显然的，因为 R 型群和 p^{∞} 型群都是递增循环群列的并集. 至于任意的阿贝尔群 G，那末如前一节所证明的，它可以嵌入一个完备群 $\bar{G}$ 内. 因此，如果 $\bar{G}$ 是某一个由循环群直和所构成的递增列的并集，则 G 是由它和这些循环群直和的交所构成的递增列的并集. 但这些交本身可以表成循环群的直和. [参看补充 28.3.]

§ 25. 纯 子 群

阿贝尔群 G 的子群 C 称为一个纯子群，如果对于 C 中的任意元素 c 和任意自然数 n，由方程

$$nx=c$$

在群 G 中可解即可推知它在子群 C 中也可解. 零子群，群 G 本身，群 G 的直被加子群及其周期部分，都是纯子群的例子.

由定义可以看出，如果子群 C 是群 G 里的纯子群，子群 C' 是 C 里的纯子群，则 C' 是 G 里的纯子群. 另一方面，一个由纯子群所构成的递增列的并集也是一个纯子群.

如果 C 是群 G 里的纯子群，则在群 $\frac{G}{C}$ 的子群和群 G 中包含 C 的子群之间的自然相互单值对应下，纯子群相互对应.

事实上，设群 G 的子群 A 包含子群 C. 如果 A 是 G 里的纯子群，并且存在一个元素 g，使

$$n(g+C)=a+C,\ \ a\in A,$$

则

$$ng=a+c\in A,$$

因而由于 A 是纯子群，在它里面可以找到一个元素 a''，使 $na''=a+c$，即

$$n(a''+C)=a+C,$$

这就证明了$\frac{A}{C}$是群$\frac{G}{C}$的一个纯子群，而且在证明中并没有用到 C 是纯子群这一事实.

现在设$\frac{A}{C}$是群$\frac{G}{C}$的纯子群，并设 G 中存在一个元素 g，使 $ng=a$，其中 $a\in A$，由此即有

$$n(g+C)=a+C,$$

因而在 A 中可找到一个元素 a'，使

$$n(a'+C)=a+C,$$

即

$$na'=a+c,\quad c\in C.$$

由此从等式 $ng=a$，可得出

$$n(a'-g)=c,$$

由于 C 是纯子群，在它里面可找到一个元素 c'，使 $nc'=c$. 这样一来就有

$$a=n(a'-c'),$$

而因为元素 $a'-c'$ 包含在 A 内，故证得 A 是 G 的纯子群.

在准素群的情形，纯子群的定义和下面的命题等价：

子群 C 是(对 p 的)准素群 G 的纯子群，当且仅当 C 中每个元素在子群 C 中和在整个群 G 中有同一高度.

事实上，用和 p 互素的任意整数来除一个元素的运算，在每一个 p^n 阶循环群里都可以进行.

下面一个更广的结果成立：

子群 C 是准素群 G 的纯子群的充分条件是：子群 C 的底层中每个元素在 C 中与在 G 中有同一高度.

事实上，假定已经证明了 C 中每个 p^n 阶元素在 G 中和在 C 中有同一高度，并设在 C 中给出了一个 p^{n+1} 阶的元素 c. 如果群 G 中存在一个元素 g，使 $p^k g = c$，则等式 $p^{k+1} g = pc$ 也成立，但因元素 pc 包含在子群 C 内，并且它的阶等于 p^n，故根据归纳假定，在 C 内可找到一个元素 c'，使 $p^{k+1} c' = pc$. 由此即有

$$p(p^k c' - c) = 0,$$

也就是说，包含在 C 内的元素 $p^k c' - c$ 的阶等于 p. 但

$$p^k c' - c = p^k (c' - g),$$

故在 C 中可找到一个元素 c''，使 $p^k c' - c = p^k c''$. 由此即有

$$c = p^k (c' - c'').$$

这就说明了元素 c 在 G 中和在 C 中的高度相等.

如果准素群 G 的纯子群 C 包含群 G 的整个底层，则 C 和 G 相重合.

事实上，如果群 G 不等于 C，则命 p^n 为 G 中不包含在 C 里的元素的最小的阶，$n>1$，并命 a 为这些元素之一. 元素 pa 已经包含在子群 C 内，但在这时由于 C 是纯子群，在它里面可以找到一个元素 c，使 $pc = pa$. 元素 $a - c$ 的阶等于 p，也就是说，属于子群 C，但这时元素 a 也会包含在 C 内.

上面已经指出，阿贝尔群的任何一个直被加子群是这个群里的一个纯子群. 这个事实的反面还不能成立. 可以证明，*如果阿贝尔群 G 可以分解成循环群的直和，并且这些被加循环子群的阶不全体有界的话，则 G 必包含一个不能作为直被加子群的纯子群* (参看 Prüfer[2]).

为了证明这一点，只限于考虑 G 是可数个循环群的直和这一情形就行了. 设这些循环群的生成元是 $a_1, a_2, \cdots, a_n, \cdots$，并设其

阶分别为 $p^{k_1}, p^{k_2}, \cdots, p^{k_n}, \cdots$，且

$$k_1 < k_2 < \cdots < k_n < \cdots.$$

我们用H表示群G中由元素 $b_1, b_2, \cdots, b_n, \cdots$所生成的子群，其中

$$b_n = a_n - p^{k_{n+1}-k_n} a_{n+1}, \quad n = 1, 2, \cdots.$$

H中的任意元素 h 具有如下的形状:

$$h = \sum_{n=1}^{N} l_n b_n = l_1 a_1 + \sum_{n=2}^{N} (l_n - l_{n-1} p^{k_n - k_{n-1}}) a_n$$

$$- l_N p^{k_{N+1} - k_N} a_{N+1}. \tag{1}$$

这个元素在G中的高度，等于能除尽等式右端生成元 $a_n(n=1,2,\cdots,N+1)$的所有系数的素数 p 的最大幂指数. 很容易看出，在这时所有系数 $l_n(n=1,2,\cdots,N+1)$也能被 p 的这个幂指数整除，因而元素 h 在子群H中和在群G中有同一高度. 这就证明了H是G的一个纯子群.

子群H中任意元素 h 的表示式(1)表明，这个子群不包含元素 a_1 的异于零的倍元. 此外，商群$\frac{G}{H}$将是一个 p^∞ 型群，因为它可由生成元 $\bar{a}_n = a_n + H$ 生成，而这些生成元适合关系式

$$p^{k_1}\bar{a}_1 = 0, \quad p^{k_{n+1}-k_n}\bar{a}_{n+1} = \bar{a}_n, \quad n = 1, 2, \cdots.$$

由此可知，子群H不能是G的直被加子群，不然的话，群G将有一个 p^∞ 型子群，而这是和前一节中所证明的循环群直和的子群定理相矛盾的. [参看补充29. 2.]

现在我们要证明两个定理，指明在怎样一些条件下一个纯子群将是一个直被加子群. 其中第一个定理可以看作是 § 19中所证明的定理——如果阿贝尔群对其某一子群的商群是自由群，则这个子群可作为一个直被加子群分解出来——的推广，因为如果一个阿贝尔群对它的某一子群的商群是无扭群的话，这个子群必是纯子群.

如果阿贝尔群 G 的子群 C 是纯子群，且商群 $\bar{G}=\frac{G}{C}$ 可分解成循环群的直和，则 C 是 G 的一个直被加子群.

事实上，设

$$\bar{G}=\sum_{\alpha}\{\bar{a}_{\alpha}\}. \tag{2}$$

从每一个陪集 $\bar{a}_\alpha$ 中可以选出这样一个代表元 a_α 来，使它的阶等于元素 $\bar{a}_\alpha$ 在群 $\bar{G}$ 中的阶．如果元素 $\bar{a}_\alpha$ 的阶是无限的，那末这是很显然的；如果元素 $\bar{a}_\alpha$ 的阶是有限的且等于 n，而 a'_α 是陪集 $\bar{a}_\alpha$ 中任意一个元素，则元素 na'_α 将包含在 C 内；这时，由于 C 是纯子群，在它里面可找到一个元素 c，使满足等式 $nc=na'_\alpha$．这就可以取元素 $a'_\alpha-c$ 作为元素 a_α，这个元素显然包含在陪集 $\bar{a}_\alpha$ 内.

我们用 A 表示群 G 中由所有元素 a_α 所生成的子群．子群 A 和 C 一道生成整个群 G，而它们的交则等于零．事实上，如果这个交里包含元素 c，

$$c=k_1a_{\alpha_1}+\cdots+k_na_{\alpha_n},$$

则在群 $\bar{G}$ 里等式

$$k_1\bar{a}_{\alpha_1}+\cdots+k_n\bar{a}_{\alpha_n}=0$$

成立；由于(2)从这个等式可得出 $k_i\bar{a}_{\alpha_i}=0,\ i=1,2,\cdots,n$．但由此即可得出 $k_ia_{\alpha_i}=0,\ i=1,2,\cdots,n$，因而 $c=0$．这就证明了直分解

$$G=C+A$$

存在.

下面的定理(Prüfer[2]，Куликов[1])在今后要不止一次地用到.

如果阿贝尔群 G 里的纯子群 C 是一个周期群，并且 C 里面的元素的阶全体有界，则 C 是 G 的一个直被加子群.

事实上，设子群 C 中所有元素的阶都是整数 n 的因子．我们用 nG 表示群 G 中能在这个群内被整数 n 所整除的元素的集合．很

容易看出这个集合是一个子群. 子群 C 和 nG 的交等于零: 这个交里的每一个元素都能在 G 中被 n 整除，因而也应该在纯子群 C 里被 n 整除，而在 C 内任意一个元素的 n 倍都等于零. 这样一来，子群 C 和 nG 就构成群 G 里的一个直和，这个直和我们记作 H,

$$H = C + nG. \tag{3}$$

现在让我们考虑商群 $\bar{G} = \frac{G}{nG}$，并证明 $\bar{G}$ 的子群 $\bar{H} = \frac{H}{nG}$ 是一个纯子群. 首先注意，群 $\bar{G}$ 里每一个元素的阶都是 n 的因子，而 $\bar{H}$ 中的每一个元素都能写成 $c + nG$ 这种形式，其中 $c \in C$. 现在设元素 $c + nG$ 在群 $\bar{G}$ 中可被 k 整除，

$$k(g + nG) = c + nG,$$

并且可以只考虑 k 是 n 的一个因子: $n = kk'$ 的情形. 从这里即有

$$kg = c + ng',$$

从而

$$c = k(g - k'g').$$

由于 C 是纯子群，在它里面可以找到一个元素 c'，使 $kc' = c$，因而

$$k(c' + nG) = c + nG,$$

这就证明了 $\bar{H}$ 是群 $\bar{G}$ 里的一个纯子群.

因为商群 $\frac{\bar{G}}{\bar{H}}$ 中所有元素的阶全体有界，它可以分解成有限多个准素群的直和，而根据 Prüfer 第一定理(见前节)，每个准素群又可分解成循环群的直和，因此，如以上所证，$\bar{H}$ 将是 $\bar{G}$ 的一个直被加子群:

$$\bar{G} = \bar{H} + \bar{F}. \tag{4}$$

我们用 F 表示子群 $\bar{F}$ 在群 G 中的原象，也就是说，$\bar{F} = \frac{F}{nG}$，由(4)可知，

$$\{H, F\} = G,\quad H \cap F = nG,$$

因而，考虑到(3)，

$$\{C, F\} = G, \quad C \cap F = 0,$$

也就是说，

$$G = C + F,$$

这就是所要证明的.

从这个定理可以推出一系列有趣的结论(参看 Куликов[1])，其中有几个我们将要在§29 里提到[参看补充 29.5.]现在我们证明下面的预备定理 (Prüfer[2]).

预备定理： *如果(对 p 的)准素群 G 中的元素 a 具有阶 p 和有限高度 n，则这个元素包含在群 G 的一个 p^{n+1} 阶直被加循环子群内.*

事实上，设 b 是这样一个元素，它使得 $p^n b = a$. 子群$\{b\}$的底层即子群$\{a\}$，并且$\{a\}$中每一个元素在$\{b\}$里和在 G 里有相同高度. 由此根据以上所证，可知$\{b\}$是群 G 里的一个纯子群，而因为在这里可以应用上面的定理，故$\{b\}$是群 G 的一个直被加子群.

从这里可以得出下面的结果.

任何不可分解的准素群或者是循环群，或者是一个 p^∞ 型群.

事实上，如果这个群 G 底层中的每一个元素在它里面都有无限高度，则如前一节中所证，G 将是一个完备群，因而由于它的不可分解性，它将是一个 p^∞ 型群. 如果在群 G 的底层中至少包含一个有限高度元素，则如刚才所证，群 G 有一个直被加循环子群，因而由于 G 的不可分解性，它本身是一个循环群.

因此，若一准素群不是循环群与 p^∞ 型群的直和，它就不能被分解成不可分解群的直和.

§26. 不含无限高度元素的准素群

可分解成循环群直和的准素阿贝尔群不包含无限高度元素.

事实上，我们知道，一个直和中的元素的高度等于这个元素的各个分支的最小高度，但循环群中每个元素的高度都是有限的. Prüfer 第二定理(参看 § 24)告诉我们，在可数群的情形，循环群的直和已穷尽了所有不含无限高度元素的准素群. 在不可数的情形，相应的定理不成立. Prüfer[1] 本人曾用一个非常复杂的例子证明了这一点，在 Ulm[2]和 Курош[9]的论文中可以找到比较简单的例子. 我们在这里介绍这些例子中的最后一个.

首先定义群 $K_n, n=1,2,\cdots$. 它的元素是序列

$$(\alpha_1, \alpha_2, \cdots, \alpha_k, \cdots), \tag{1}$$

这里 α_k 是满足条件 $0 \leqslant \alpha_k < p^n$ 的整数. 我们还进一步要求 α_1 被 p^{n-1} 整除，α_2 被 p^{n-2} 整除，…，α_{n-1} 被 p 整除. K_n中的群运算被认为是序列(1) 的对应元素相加，再按模 p^n 约化. 完全由零组成的序列是零元素. 群K_n 具有连续统的势并且是准素的，它的元素的阶是 p^n 的因子.

如果对于群K_n 的每一个元素(1)，令群 K_{n+1} 的元素

$$(p\alpha_1, p\alpha_2, \cdots, p\alpha_k, \cdots) \tag{2}$$

与它对应——序列(2)显然，满足对群 K_{n+1} 的元素所提出的全部要求，——那么就得到群 K_n 到群 K_{n+1} 内的一个同构映射. 因此，在上述的同构嵌入之下，群 $K_n, n=1,2,\cdots$，作成一个递增序列；它们的并集记作 K.

我们证明，*群 K 不含无限高度的元素*. 事实上，K_n 中每一个在 K_{n-1} 之外的元素 a 的阶等于 p^n. 然而这样一来，元素 $p^{n-1}a$ 就将是 K_1 中的元素，在它的形如(1)的序列的写法里，前 $n-1$ 个位置都是零. 由此推出，在群K的底层 K_1 里，没有在群K内具无限高度的元素. 因此，这样的元素也不可能在群K内.

现在证明，*群 K 不可能分解成循环群的直和*. 假设它真有这样的分解. 从这些分解中选取一个，并且用 H^k 表示这个分解中所有

阶为p^k的循环直被加群的直和. 如果H_1^k是子群H^k的底层,那末子群K_1将是所有子群H_1^k的直和,又因为K_1有连续统的势,所以子群H_1^k中,$k=1,2,\cdots$,至少有一个应该是无限的. 换句话说,如果引入记号

$$F_n=\sum_{k=n}^{\infty}H_1^k,$$

那末至少对某一个n来说,子群F_{n+1}在子群F_n里应该具有无限指数. 然而,容易看出,子群F_n恰由子群K_1中这样的元素所组成,它们在群K中的高度不小于$n-1$,也就是说,恰由K_1中这样的元素所组成,在它们写成形如序列(1)的写法里,前$n-1$个位置都是零. 由此推出,对于任意n,子群F_{n+1}在子群F_n内的指数是有限的并且等于p. 这与上面所证明的论断相矛盾.

在 Куликов[1,2]的论文中甚至还证明了,对于任意不可数势$\mathfrak{M}$,可找出一个准素群来,使它具有这一势,不包含无限高度元素,也不能作这样一种直分解,其中所有被加子群的势都不超过某一小于$\mathfrak{M}$的势$\mathfrak{M}'$. 另一方面,Куликов[2]也对不含无限高度元素的准素群作了某种描述,这种描述不是完全的,可是已经足以证明Prüfer第二定理不能推广到不可数的情形. 现在我们就来论述 Куликов 的这一理论.

准素阿贝尔群G的子群B称为一个*基子群*,如果它是G里的一个纯子群并且可分解成循环群的直和,而商群$\frac{G}{B}$是一个完备群. 例如在任何一个完备准素群中,零子群是唯一的基子群。另一方面,准素(对p)循环群的任何直和是它本身的基子群,而在群中元素的阶全体有界的情况下,甚至还是唯一的基子群.

任何一个准素阿贝尔群G都具有基子群.

根据上面对完备群的基子群所作的说明,可以把G看作一个

非完备群. 因此(参看§24),群G中存在有限高度的p阶元素,而根据上节结尾处所证的预备定理,这种元素可嵌入一些直被加循环群内. 因此,群G含有元素的阶全体有界的纯子群. 由这个事实,以及由递增纯子群列的并集仍是纯子群的事实可知,在群G里可以找到一个递增子群列

$$B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n \subseteq \cdots, \tag{3}$$

使具有下面的性质:

1) 每个子群$B_n(n=1, 2, \cdots)$都是G里的纯子群;

2) B_n中元素的阶不大于p^n;

3) 子群B_n不能嵌入一个同样具有性质1)和2)的更大的子群内.

用B表示子群列(3)的并集. 作为递增纯子群列的并集,这个子群是群G的一个纯子群. 除此之外,Куликов的判定法(参看§24)告诉我们,子群B可分解成循环群的直和,因为从$B_n(n=1, 2, \cdots)$是纯子群以及它的所有元素的阶都有界这事实,可知这些元素在群G中的高度都是有限的,而且全体有界.

现在我们证明商群$\frac{G}{B}$是完备群. 由§24,我们知道,要证明这一点,只要证明这个商群的每一个阶为p的陪集$x+B$在它里面有无限高度就行了. 根据条件,$px \in B$. 但因B是纯子群,故在它里面可以找到一个元素b,使$pb=px$,由此即有$p(x-b)=0$. 因此我们可以把x本身看作群G中的一个p阶元素,也就是说,$px=0$.

子群$B_n(n=1, 2, \cdots)$是G里的纯子群,其元素的阶不超过p^n. 因此,如前一节中所证,存在一个直分解

$$G=B_n+C_n, \quad n=1, 2, \cdots, \tag{4}$$

与此相应,元素x可分解成两个元素之和

$$x=y+z,$$

其中 $y\in B_n$, $z\in C_n$. 因为 x 不包含在子群 B 内，故元素 z 不等于零，因而 z 的阶等于 p. 元素 z 在群 G 中的高度不小于 n. 事实上，如果它的高度小于 n 的话，那末根据前一节中的预备定理，元素 z 就可以嵌入群 C_n 的一个阶不大于 p^n 的直接被加循环子群内. 由于(4)，这就会引出和子群 B_n 的性质 3) 相矛盾的结果. 但元素 $z=x-y$ 包含在陪集 $x+B$ 内，故这个陪集包含高度任意大的元素，因而陪集 $x+B$ 在群 $\frac{G}{B}$ 中的高度是无限的.

这样就证明了子群 B 是群 G 的一个基子群.

准素阿贝尔群 G 的所有基子群彼此同构.

设 B 是群 G 中一个任意的基子群. 从 §24中我们知道，所有将群 B 分解成循环群的直分解是彼此同构的. 在每一个这样的直分解中，p^k $(k=1, 2, \cdots)$ 阶被加群的个数(这种被加群的集合的势)显然等于商群 $\frac{B}{p^nB}$ $(n>k)$ 的分解中 p^k 阶被加循环群的个数，而 p^nB 则是由群 B 中高度大于或等于 n 的所有元素所组成的子群. 因此如果我们能够证明商群 $\frac{B}{p^nB}$ 和基子群 B 的选择无关，那末我们的定理就被证明了.

我们用 p^nG 表示群 G 中高度(在 G 中)大于或等于 n 的所有元素所组成的子群. 由于 B 是纯子群，可得出等式

$$B\cap p^nG=p^nB. \tag{5}$$

另一方面，

$$\{B, p^nG\}=G. \tag{6}$$

事实上，如果 x 是群 G 中一个任意元素，那末由商群 $\frac{G}{B}$ 的完备性，可知群 G 中存在这样一个元素 y，使得元素 x 和 p^ny 包含在 G 对 B 的同一陪集内，也就是说，$x=p^ny+b$.

根据等式(5)和(6)，关于同构的定理(§10)导致下面的同构

关系:

$$\frac{B}{p^nB} \simeq \frac{G}{p^nG}.$$

这样,当 n 给定时,对于群 G 的一切基子群 B 来说,商群 $\frac{B}{p^nB}$ 彼此同构. 定理证毕. [参看补充 30.1.]

现在让我们应用所得出的结果来研究不含无限高度元素的准素群. 我们看到,如果把这些群中基子群相互同构的群归作一类的话,那我们就能够把这些群分成许多彼此不相交的类. 在这种分类方法下,凡可以分解成循环群直和的准素群决定一个类,因为它可以作为它本身的基子群. 这样一来,描述全部不含无限高度元素的准素群的问题,就归结为描述具有已知基子群 B 的群的问题.

为了这个目的,我们引入一个新的概念. 取群 B 的一个循环群直分解,并用 $B^{(n)}$ $(n=1, 2, \cdots)$ 表示这一分解中 p^n 阶被加群的直和;如果没有这一阶的被加群,那就命 $B^{(n)}=0$. 其次,我们作所有群 $B^{(n)}$(在 §17结尾处的意义下)的完全直和,并且称这个和的周期部分为群 B 的闭包,记作 $\bar{B}$. 换句话说,群 $\bar{B}$ 中的元素是由每一个群 $B^{(n)}$ 中各取出一个元素所构成的元素列,并且每个元素列中所有元素的阶全体有界;元素列的相加按分支进行.

因为群 B 的所有分成循环群的直分解彼此同构,故群 $\bar{B}$ 由群 B 唯一决定. 容易看出,群 $\bar{B}$ 是准素的,并且不包含无限高度的元素. 群 B 是群 $\bar{B}$ 中的一个子群,它由 $\bar{B}$ 中仅含有有限多个不等于零的元素的元素列所组成. 因此,群 B 和其闭包相重合,当且仅当 B 中元素的阶全体有界;因为在这一情形,并且只有在这一情形,才仅有有限多个群 $B^{(n)}$ 不为零.

在一般的情形下,群 B 是其闭包 $\bar{B}$ 的基子群.

事实上,群 B 可分解成循环群直和这一点已预先假定. 为了证明它是群 $\bar{B}$ 中的纯子群,我们注意和 $C^{(n)}=B'+B''+\cdots+B^{(n)}$ $(n$

$=1,2,\cdots$)是群$\bar{B}$的一个直被加子群，与之相补的被加子群是由前 n 个分支等于零的元素列所组成的子群. 因此，由于群B是$\bar{B}$的纯子群 $C^{(n)}$所构成的递增列的并集，故本身是一个纯子群. 最后，我们证明商群$\frac{\bar{B}}{B}$的完备性. 如果$x=(x_1, x_2, \cdots, x_n, \cdots)$是群$\bar{B}$中一个任意元素，则因为它的各个分支的阶全体有界，对任意 k 可找到一个N，使对所有 $n(n\geqslant N)$元素 x_n 在相应的群 $B^{(n)}$中的高度不小于 k. 由此即可知元素 $x'=(0, \cdots, 0, x_N, x_{N+1}, \cdots)$在$\bar{B}$中的高度也不小于 k. 但元素 x' 属于陪集 $x+B$，故这个陪集包含高度任意大的元素，因而它在商群$\frac{\bar{B}}{B}$中的高度是无限的.

现在我们可以指出：*存在不能分解成循环群直和的不含无限高度元素的准素群.*

事实上，设B——可分解成循环群直和的准素群——是一个可数群，但包含阶为任意大的元素. 这样，它的闭包$\bar{B}$就具有连续统的势. 群$\bar{B}$不能分解成循环群的直和，因为不然的话，$\bar{B}$里就会有两个不同构的基子群：$\bar{B}$本身和群B；而这与前面所证明的关于一个准素群中所有基子群彼此同构的定理相矛盾.

凡基子群和群B同构且又不含无限高度元素的所有准素群，都不外乎是群$\bar{B}$—群B的闭包—中那样的一些子群，这些子群包含B并且它们在商群$\frac{\bar{B}}{B}$中的象是完备子群.

事实上，设$\frac{C}{B}$是群$\frac{\bar{B}}{B}$的任意一个完备子群. 群C作为群$\bar{B}$的一个子群将是一个不含无限高度元素的准素群，子群B包含在C内，并且是它的一个基子群——由B是$\bar{B}$的纯子群可知B是C中的纯子群，而商群$\frac{C}{B}$的完备性则已事先假定. 因此，群C属于我们所考虑的这一类群.

现在设G是任意一个不含无限高度元素的准素群，并设其基子群与群B同构. 我们从它的基子群中挑选出一个，并将它记作B_0. 我们知道，B有直分解

$$B=\sum_{n=1}^{\infty}B^{(n)},$$

其中$B^{(n)}$是p^n阶循环群的直和. 因此

$$B_0=\sum_{n=1}^{\infty}B_0{}^{(n)},$$

且$B_0^{(n)}\simeq B^{(n)}$. 引入记号

$$D^{(k)}=\sum_{n>k}B_0{}^{(n)},$$

从而

$$B_0=B_0'+B_0''+\cdots+B_0^{(k)}+D^{(k)},$$

并且命

$$G^{(k)}=\{D^{(k)},p^kG\},$$

其中p^kG还像前面一样，是群G中高度(在G中)不小于k的一切元素所组成的子群. 前面已经证明[参看等式(4)]，对所有$k(k=1,2,\cdots)$等式

$$G=\{B_0,p^kG\}$$

成立，因而

$$G=\{B_0'+B_0''+\cdots+B_0^{(k)},G^{(k)}\}.$$

设元素x包含在子群$B_0'+B_0''+\cdots+B_0^{(k)}$和$G^{(k)}$的交内. 作为第二个子群里的元素，$x$具有$x=y+z$的形式，其中$y\in D^{(k)}$，$z\in p^kG$. 因为$x$和$y$属于子群$B_0$，故元素$z=x-y$包含在$B_0$内. 元素$z$在$G$里的高度不小于$k$，因而它在$B_0$里的高度也不小于$k$，因为$B_0$是$G$的纯子群. 然而群$B_0$中一切高度不小于$k$的元素都属于$D^{(k)}$，因此元素$x$作为$D^{(k)}$中两个元素的和，也应该包含在$D^{(k)}$

内. 另一方面它又属于 $B_0'+B_0''+\cdots+B_0^{(k)}$，所以 x 等于零.

这样就证明了直分解

$$G=B_0'+B_0''+\cdots+B_0^{(k)}+G^{(k)},\quad k=1,2,\cdots \tag{7}$$

的存在；并且因为子群 $G^{(k)}$ 包含子群 $B_0^{(k+1)}$ 和子群 $G^{(k+1)}$，所以直分解

$$G^{(k)}=B_0^{(k+1)}+G^{(k+1)},\quad k=1,2,\cdots,$$

成立. 这就是说，如果将(7)中每个直分解中的最后一项作一次分解，就得出次一个直分解. 从这里可以看出，当 $k=n,n+1,\cdots$ 时，群 G 中每个固定的元素 x，在(7)中每个直分解的直被加群 $B_0^{(n)}$ 中有同一分支，我们把这个分支记作 x_n.

显然，对群 G 中的每个元素 x，使它的分支的序列 $(x_1,x_2,\cdots,x_n,\cdots)$ 与它相对应，我们就得到一个同态映射，将群 G 映入群 B 的闭包 $\bar{B}$——显然，所有分支 x_n 的阶都不大于元素 x 的阶，也就是说，分支序列的确包含在 $\bar{B}$ 内. 这个映射甚至还是一个同构映射，因为零序列所对应的那个元素 x 应包含在所有子群 $G^{(k)}(k=1,2,\cdots)$ 内，也就是说，它应有无限高度，因而由于群 G 中不含无限高度元素，x 应该等于零. 这个同构映射将群 G 映成群 $\bar{B}$ 中的一个子群 C，而将子群 B_0 映成子群 B: B_0 中的元素对应于只包含有限多个不等于零的分支序列，并且只有 B 中的元素对应于这样的分支序列；另一方面，每一个这样的序列都和 B_0 中一个元素相对应. 最后，由商群 $\frac{G}{B_0}$ 的完备性可知商群 $\frac{C}{B_0}$ 是完备群. 这就结束了定理的证明.

应当指出，在证明过程中所造出来的群 $\bar{B}$ 中与群 G 同构的子群 C，和群 G 中基子群 B_0 的选择有关. 至于群 $\frac{\bar{B}}{B}$ 的完备子群 $\frac{C}{B}$ 和 $\frac{C'}{B}$ 应该服从哪些条件，才能使群 $\bar{B}$ 中相应的子群 C 和 C' 同构，这

个问题现在还没有解决.

在 Куликов 的论文[2]中，可以找到表示为循环群直和的闭包的那种准素群的一系列进一步的性质. 此外还可以参看 Kaloujnine 的论文[8]. [参看补充30.2]

§ 27. Ulm 因子·存在定理

现在我们转来研究包含无限高度元素的准素阿贝尔群. 不要以为凡是包含无限高度元素的准素群都一定包含完备子群——如果准素群 G 中的元素 a 在它里面有无限高度，那末满足方程 $p^n b_n = a$ 的元素 $b_n (n=1, 2, \cdots)$ 也不一定包含在同一 p^∞ 型子群内. 本节中的基本定理将表明，既约准素群的构造——根据 § 23中的结果，在下面我们可以只考虑既约群——即使在可数的情形，也要比不含无限高度元素的准素群的构造复杂得多.

因为准素群 G 中两个无限高度元素的和与差在 G 中也有无限高度，故所有具无限高度元素的集合(加上零元)是群 G 的一个子群；这个子群我们把它记作 G^1. 我们用 G^2 表示子群 G^1 的所有在 G^1 中具有无限高度的元素所组成的子群. 一般地，如果对小于某一 β 的所有序数 α，在群 G 中都已定出了子群 G^α，并且这些子群构成一个递降序列，那末在 β 为非极限序数时，我们就命子群 $G^{\beta-1}$ 的所有在 $G^{\beta-1}$ 中具有无限高度的元素所组成的子群为 G^β；如果 β 是极限序数，则命所有子群 $G^\alpha (\alpha<\beta)$ 的交为 G^β.

这样我们就得出了群 G 的一个递降子群列:

$$G=G^0 \supset G^1 \supset \cdots \supset G^\alpha \supset \cdots,$$

这个子群列应当在某一序数 γ 上中断. 说得确切一些，就是存在这样一个序数 γ，它的势不大于群 G 本身的势，而使得 $G^\gamma = G^{\gamma+1}$，因而对所有大于 γ 的序数 δ, $G^\gamma = G^\delta$. 然而等式 $G^\gamma = G^{\gamma+1}$ 表明，子群 G^γ 中所有元素在 G^γ 中有无限高度，也就是说，子群 G^γ 是一个

完备群. 因为根据所作假定,群 G 是既约的,故子群 G^{ν} 应等于零.

设 τ 是第一个使得$G^{\tau}=0$ 的序数. 序数 τ 称为既约群 G 的型. 很显然,不含无限高度元素的群的型等于 1.

如果 G 是一个 τ 型既约准素群,则对所有小于 τ 的序数α, 我们作商群

$$\overline{G}^{\alpha}=\frac{G^{\alpha}}{G^{\alpha+1}}.$$

群列

$$\overline{G}^{0},\ \overline{G}^{1},\ \cdots,\ \overline{G}^{\alpha},\ \cdots,\ \alpha<\tau$$

称为群 G 的 Ulm 因子列. 从这个因子列的构造过程可以看出,它是由群 G 本身所唯一决定的, 并且子群 $G^{\alpha}(\alpha<\tau)$ 的 Ulm 因子列将是

$$\overline{G}^{\alpha},\ \overline{G}^{\alpha+1},\ \cdots,\ \overline{G}^{\beta},\ \cdots,\ \alpha\leqslant\beta<\tau.$$

Ulm因子对准素群理论的意义将在下面, 特别是在下一节中看出来.

在证明 Ulm 因子的一些最简单的性质时,将要用到下面的注记. 设准素群 G 被同态地映成准素群 H, 并且被映成群H 中零元的是群 G 中这样一个子群 A, 它里面所有元素在群 G 中都有无限高度. 那末群 G 中每一个不属于 A 的无限高度元素的象都是 H 里的无限高度元素;反之, H 里一个无限高度元素的每一个原象都是 G 里的无限高度元素. 第一个论断可由同态映射的定义直接推出. 现在我们证明第二个论断. 设 h 是 H 中的一个无限高度元素, g 是 h 在 G 中的一个原象. 如果 $p^{n}h'=h, h'\in H$, 而 g' 是元素 h' 在 G 中的一个原象, 那末

$$p^{n}g'=g+a,\ a\in A.$$

根据我们对子群 A 所作的假定, 在群 G 中可以找到一个元素b, 使 $p^{n}b=a$. 由此即有

$$p^n(g'-b)=g,$$

因而元素 g 在群 G 中有无限高度.

特别，从这个注记可知，准素群 G 的所有 Ulm 因子都是不含无限高度元素的群. 为了证明这一点，只要将这个注记应用到将群 G^α 映成商群 $\frac{G^\alpha}{G^{\alpha+1}}=\overline{G}^\alpha$ 的自然同态映射上就行了.

我们还可以证明，群 $F=\frac{G}{G^\sigma}(\sigma\leqslant\tau)$ 是一个 σ 型准素群，并且它的 Ulm 因子列是：

$$\overline{G}^0, \overline{G}^1, \cdots, \overline{G}^\alpha, \cdots,\quad \alpha<\sigma.$$

事实上，我们考虑将群 G 映成群 F 的自然同态映射. 由上述可知，在这个同态映射之下，子群 G^1 被映成子群 F^1，但因为 $G^1\supseteq G^\sigma$，故根据在同态映射下子群相对应的定理，子群 $\frac{G}{G^1}=\overline{G}^0$ 与 $\frac{F}{F^1}=\overline{F}^0$ 同构. 设对小于 β 的所有 α，已经证明了子群 G^α 在这个映射下被映成 F^α. 如果 $\beta-1$ 存在，则如上面一样，我们可以得出 G^β 被映成 F^β，且 $\overline{G}^{\beta-1}\simeq\overline{F}^{\beta-1}$；如果 β 是一个极限序数，则 G^β 仍旧被映成 F^β，因为前者是所有子群 $G^\alpha(\alpha<\beta)$ 的交，而后者则是这些子群的象的交.

如果准素群 G 是群 H_ν 的直和，$G=\sum\limits_\nu H_\nu$，则对小于群 G 的型的每个序数 α，

$$\overline{G}^\alpha=\sum_\nu \overline{H}_\nu^\alpha.$$

当然，在这里须假定，如果 α 大于或等于群 H_ν 的型的话，$\overline{H}_\nu^\alpha=0$.

我们将要证明，对于任意 β，子群 G^β 是所有子群 H_ν^β 的和(并且显然是直和). 假定这个命题对小于 β 的所有 α 已被证明(当 $\beta=0$ 时它是正确的). 如果 $\beta-1$ 存在的话，则 $G^{\beta-1}=\sum\limits_\nu H_\nu^{\beta-1}$，因

而 H^{β} 中的每一个元素在 $G^{\beta-1}$ 中都有无限高度，也就是说，$G^{\beta}\supseteq\sum_{\nu}H_{\nu}^{\beta}$. 另一方面，如果 g 是 $G^{\beta-1}$ 中任意一个无限高度元素，且 $g=\sum_{\nu}h_{\nu}$, $h_{\nu}\in H_{\nu}^{\beta-1}$，则每个元素 h_{ν} 在 $H_{\nu}^{\beta-1}$ 内应该有无限高度，由此即有 $G^{\beta}\subseteq\sum_{\nu}H_{\nu}^{\beta}$，因此，$G^{\beta}=\sum_{\nu}H_{\nu}^{\beta}$，于是由直和的定义很容易得出

$$\overline{G}^{\beta-1}=\frac{G^{\beta-1}}{G^{\beta}}\simeq\sum_{\nu}\frac{H_{\nu}^{\beta-1}}{H_{\nu}^{\beta}}=\sum_{\nu}\overline{H}_{\nu}^{\beta-1}.$$

如果 β 是一个极限序数，那末我们的命题可以由子群 G^{β} 是所有子群 $G^{\alpha}(\alpha<\beta)$ 的交这一事实推出.

直到目前为止，我们都是从准素群的型及其 Ulm 因子的定义出发来讨论问题的，还没有注意到是否任何一个序数都能作为某一个准素群的型，以及会不会发生这样一种情况，例如子群列 $G\supset G^{1}\supset\cdots\supset G^{\alpha}\supset\cdots$ 永远在一个有限的位置上中断的问题. 此外，我们也不知道，一个由不含无限高度元素的准素群所构成的群列，应该具有怎样一些性质，才能作为一个准素群的 Ulm 因子列. Куликов 对这些问题给了一个完满的答复. 可是这个答案是非常复杂的，因此在以下我们只限于对可数准素群来加以讨论.

我们知道，如果 G 是一个可数的既约准素群，那末它的型 τ 具有限或可数的势. 这个群的 Ulm 因子将是一些不含无限高度元素的可数群，因而根据 Prüfer 第二定理，它们可以分解成循环群直和. 其次，还可以断言(并且在这里群的可数性并不起作用)，在所有 Ulm 因子中，可能要除去因子 $\overline{G}^{\tau-1}$ 外 (如果 $\tau-1$ 存在的话)，元素的阶不全体有界. 事实上，如果 $\alpha<\tau-1$，则 $G^{\alpha+1}\neq 0$，因而在这个子群里可以找到一个元素，使它在这个子群中的高度为有限，虽然它在 G^{α} 中的高度是无限的.

下面的定理表明，这里所建立的 Ulm 因子的必要性质，在可数的情形也是充分的(见 Zippin[1][1]).

设给定一个序数 τ，其势不大于可数，而对每个序数 $\alpha(0\leqslant\alpha<<\tau)$ 都给出了一个不包含无限高度元素的可数准素群 A_α，并且对所有 α，可能要除去 $\alpha=\tau-1$ 的情形外(如果 τ 是非极限序数的话)，群 A_α 包含阶为任意大的元素．在这样的条件下，一定存在一个可数的既约准素群，具有型 τ 并且以群列

$$A_0, A_1, A_2, \cdots, A_\alpha, \cdots, \alpha<\tau$$

为其 Ulm 因子列.

证明　根据 Prüfer 第二定理，每一个群 A_α 可分解成循环群的直和．设这些循环群的生成元是

$$a_{\alpha 1}, a_{\alpha 2}, \cdots, a_{\alpha i}, \cdots,$$

且元素 $a_{\alpha i}$ 的阶是 $p^{n_{\alpha i}}$．我们用下面的方法来定义一个群 G: G 的生成元是与元素 $a_{\alpha i}$ (其中 α 取小于 τ 的一切可能的值)一一对应的元素 $c_{\alpha i}$．对每个元素 $c_{\alpha i}$，或者使等式 $p^{n_{\alpha i}}c_{\alpha i}=0$，或者使等式 $p^{n_{\alpha i}}c_{\alpha i}=c_{\beta j}$ 和它相对应，其中 $\beta>\alpha$，并将所得出的等式连同可换性关系一道作为群 G 的定义关系．此外还要求满足下面的条件:

1) 设给定一元素 $c_{\alpha i}$，如果和它相对应的关系是 $p^{n_{\alpha i}}c_{\alpha i}=c_{\alpha_1 i_1}$，而和 $c_{\alpha_1 i_1}$ 相对应的关系是 $p^{n_{\alpha_1 i_1}}c_{\alpha_1 i_1}=c_{\alpha_2 i_2}$ 等等，那末经过有限多步之后，可得到一个元素 $c_{\alpha_k i_k}$，使相应的关系是 $p^{n_{\alpha_k i_k}}c_{\alpha_k i_k}=0$.

2) 如果任意给定一个元素 $c_{\beta j}$，$\beta>0$，一个小于 β 的序数 γ 和一个自然数 N，那末一定存在一个元素 $c_{\alpha i}$，使 $\gamma\leqslant\alpha<\beta$，$n_{\alpha i}>N$，而相应的关系具有 $p^{n_{\alpha i}}c_{\alpha i}=c_{\beta j}$ 的形式.

3) 如果 τ 是极限序数，那末对于任意小于 τ 的序数 γ 和任意

1) 但 Zippin 的论文中并没有这个定理的完善证明.

自然数N，一定存在一个元素$c_{\alpha i}$，使$\gamma<\alpha, n_{\alpha i}>N$，而相应的关系具有$p^{n_{\alpha i}}c_{\alpha i}=0$的形式.

现在我们要证明，满足这三项要求的一组等式的确是存在的，并且这样定义出来的群G满足定理中的条件. 这可以对序数τ进行归纳法来证明. 事实上，当$\tau=1$时，群G由生成元$c_{01}, c_{02}, \cdots, c_{0i}$和关系$p^{n_{0i}}c_{0i}=0$所定义，因而条件1)—3)满足，而群$G$与群$A_0$同构.

先假设序数$\tau-1$存在. 设G'是一个$\tau-1$型群，其Ulm因子列为

$$A_0, A_1, A_2, \cdots, A_\alpha, \cdots, \alpha<\tau-1;$$

并设这个群由生成元$c_{\alpha i}(\alpha<\tau-1)$及和这些生成元相应的上述类型的关系所决定，且条件1)—3)满足. 群G中的关系我们按下述方式来定义：如果在群G'中和元素$c_{\alpha i}(\alpha<\tau-1)$相应的关系式是$p^{n_{\alpha i}}c_{\alpha i}=c_{\beta j}(\beta<\tau-1)$那末在群$G$中和它相应的也是这个关系. 如果在群$G'$中和元素$c_{\alpha i}(\alpha<\tau-1)$相应的关系是$p^{n_{\alpha i}}c_{\alpha i}=0$，那末在群$G$中这个关系换成$p^{n_{\alpha i}}c_{\alpha i}=c_{\tau-1,j}$这种形式的关系. 容易看出，在这里还可以作到使条件2)对元素$c_{\tau-1,i}$成立——这是由于，元素$c_{\tau-1,i}$不超过可数多个，在$\tau-1$为极限序数时可利用条件3)，而在$\tau-1$不为极限序数时可利用这样的事实，即存在具有任意大指数$n_{\tau-2,i}$的元素$c_{\tau-2,i}$，而在G'中和所有元素$c_{\tau-2,i}$相应的关系都具有$p^{n_{\tau-2,i}}c_{\tau-2,i}=0$的形式. 最后，对于元素$c_{\tau-1,i}$我们使关系$p^{n_{\tau-1,i}}c_{\tau-1,i}=0$和它们相应. 这样我们就得出一组满足条件1)和2)的定义关系. 在这一情形，条件3)是不起作用的.

由1)可以看出，这样构造的阿贝尔群G是一个准素群. 我们证明，这个群中所有元素$c_{\alpha i}(\alpha<\tau)$都不等于零. 事实上，取元素$c_{\alpha i}$并写出关系式

$$p^{n_{\alpha i}}c_{\alpha i}=c_{\alpha_1 i_1},\quad p^{n_{\alpha_1 i_1}}c_{\alpha_1 i_1}=c_{\alpha_2 i_2}, \cdots,$$

$$\cdots, p^{n_{\alpha_k i_k}} c_{\alpha_k i_k} = c_{\tau-1,j}, \quad p^{n_{\tau-1,j}} c_{\tau-1,j} = 0$$

——由我们构造群G的方法可以看出，这样做下去我们一定能够达到一个元素$c_{\tau-1,j}$. 引入记号

$$n_{\alpha i} + n_{\alpha_1 i_1} + \cdots + n_{\alpha_k i_k} + n_{\tau-1,j} = l(\alpha, i).$$

其次，作p^∞型群P，命其生成元为$d_1, d_2, \cdots, d_n, \cdots$,

$$pd_1 = 0, pd_n = d_{n-1}, \quad n = 2, 3, \cdots.$$

如果对每个元素$c_{\alpha i}$，我们使群P中的元素$d_{l(\alpha,i)}$与它对应，那末很容易看出，群G中所有定义关系在P中都能满足，并且群P中与所有元素$c_{\alpha i}$相对应的元素都不等于零. 这就证明了由群G的定义关系不能推出任何一个元素$c_{\alpha i}$等于零. 除此之外，我们还得出，群G中每个元素$c_{\alpha i}$的阶等于$p^{l(\alpha,i)}$.

现在已经可以对α进行归纳，并且利用条件2)来证明每个元素$c_{\alpha i}$包含在像本节开始所述那种方法定义的子群G^α内. 特别，所有元素$c_{\tau-1,i}$属于子群$G^{\tau-1}$. 如果F是群G中由所有元素$c_{\tau-1,i}$所生成的子群，那末商群$\frac{G}{F}$与群G'同构. 因为G'的型为$\tau-1$，故从这里可以看出，群G中除F中的元素外，没有其他属于$G^{\tau-1}$的元素，也就是说，$F = G^{\tau-1}$. 因此

$$\overline{G}^\alpha \simeq \overline{G}'^\alpha \simeq A_\alpha, \quad \alpha < \tau - 1.$$

至于子群$G^{\tau-1}$，则它是循环群$\{c_{\tau-1,i}\}$的直和，因而与群$A_{\tau-1}$同构. 这一点可由下面的事实得出：即正如定义关系所指出的，群G本身就是这样一些子群的直和，这些子群的每一个都是由这样的一些元素$c_{\alpha i}$生成的，它们的循环子群包含固定元素$c_{\tau-1,j}$. 因此群G满足定理的全部条件.

现在假定τ是一个极限序数. 每一个群$A_\alpha (0 \leqslant \alpha < \tau)$都是一些循环群的直和，这些循环群的阶不全体有界. 这就可能把A_α分解成可数个子群的直和，其中每一子群都含有任意高阶的元素. 设

这一分解是

$$A_\alpha = A_{\alpha\alpha} + A_{\alpha,\alpha+1} + \cdots + A_{\alpha\sigma} + \cdots, \quad \alpha \leqslant \sigma < \tau^{1)}.$$

根据归纳假定,存在一个 $\alpha+1$ 型群 H_α,以序列

$$A_{0\alpha}, A_{1\alpha}, A_{2\alpha}, \cdots, A_{\alpha\alpha}$$

为其 Ulm 因子列. 我们知道,一切群 $H_\alpha(0\leqslant\alpha<\tau)$的直和已满足定理的全部条件. 同时,将群 H_α 中相应的生成系合并在一起, 并且保持这些群中相应的关系, 就得出这个直和的生成系 $c_{\alpha i}$. 显然,条件1)和 2)都被满足. 又因为每一个子群 $A_{\alpha\alpha}(0\leqslant\alpha<\tau)$都包含任意高阶的元素,所以条件3)也成立.

这就结束了定理的证明. [参看补充30.3.]

§ 28. Ulm定理

上一节的基本定理表明,即使在可数的情形下,既约准素群已可能是非常多种多样的了——任意一个具有可数势的序数都可以作为这样群的型,而任意一个不含无限高度元素的(并适合一个非常自然的限制的)可数准素群序列都可以作为这个群的 Ulm 因子列. 然而,在实际上, 群的 Ulm 因子和型不但可以用来确定我们所考虑的这种群的多样性, 而且还可以用来对这样的群作出完全的描述. 为了这个目的,我们证明以下定理.

Ulm定理. *若可数既约准素群 A 与 B 有同一型τ,且对任何小于 τ 的α,它们的 Ulm 因子$\overline{A}^\alpha$与$\overline{B}^\alpha$同构,那末群 A 与 B 彼此同构.*

这个定理是由 Ulm[1]引用了无限矩阵的理论证明而由 Zippin[1]用群论的方法重新加以证明的. 显然, 这个定理断言, 任何可数既约准素群可以由它的型以及它的 Ulm 因子列的给出而完全确定,但因为根据 Prüfer 第二定理,在可数情形下,任意Ulm

1) 显然,这里我们可以随意编号.

因子都可以分解成为循环群的直和，因而由其 p^n(对任意n) 阶的直被加群的个数完全确定，所以就使得我们有可能用一组整数不变量来给出可数准素群. 自然，这一组整数不变量比起用来给出一个具有限生成系的阿贝尔群的不变量来要更为复杂.

设

$$A=A^0\supset A^1\supset A^2\supset\cdots\supset A^\alpha\supset\cdots\supset A^\tau=0$$

是群A中按前一节的方式定义的子群列: 如果 $\alpha-1$ 存在,那末 A^α 是 $A^{\alpha-1}$中一切具无限高度元素所成的子群,如果α是极限数,那末 A^α 是所有 $A^\beta(\beta<\alpha)$的交. 相应地,作出序列

$$B=B^0\supset B^1\supset B^2\supset\cdots\supset B^\alpha\supset\cdots\supset B^\tau=0.$$

群A的元素a 叫做一个 α 型元素,假如它包含在子群 A^α 中但不在子群 $A^{\alpha+1}$ 中. 群A的任意元素都具有某一型: 如果所给的元素包含在所有子群 A^β 内,此处β小于极限序数α,那末它也包含在这些子群的交内,即包含在 A^α 内.

其次,设X是群A的子群且$\alpha<\tau$. 交$X\cap A^\alpha$是群 A^α 的子群; 设在群 A^α 到 Ulm 因子$\bar{A}^\alpha=\frac{A^\alpha}{A^{\alpha+1}}$上的自然同态映射之下，这个交被映成群 $\bar{A}^\alpha$ 的子群 $\bar{A}^\alpha_X$. 子群X叫做群A的一个完全子群，假如对于任意α,子群 $\bar{A}^\alpha_X$ 都是群 $\bar{A}^\alpha$ 的纯子群(关于纯子群的定义可参看§25).

显然,关于元素的型和完全子群的定义也可以转移到群B上.

最后,我们引入以下定义: 假设在群A和群B中已经选出彼此同构的子群X与Y; 如果这两个子群之间的同构φ使得X和Y中分别在A和B中具有相同型的元素彼此对应，那末φ就叫作一个保型同构.

下面的预备定理构成 Ulm 定理的证明中最基本的部分.

设在群A与B中分别给定彼此同构的有限完全子群X与Y，而φ是它们之间的保型同构. 其次，设群A中元素a不包含在X

内. 那末在群 A 中可以找到一个包含 X 及 a 的有限完全子群 $\overline{X}$，而在 B 中可以找到一个包含 Y 的有限完全子群 $\overline{Y}$，使得 $\overline{X}$ 与 $\overline{Y}$ 彼此同构，并且在它们之间存在一个保型同构 $\overline{\varphi}$，而 $\overline{\varphi}$ 是同构 φ 的延拓.

首先注意，可以只限于讨论 $pa\in X$ 的情形：$p^n a\in X$，但 $p^{n-1}a\notin X$，$n>1$，的情形可以归结到所指出的特殊情形，因为我们可以把元素 $p^{n-1}a, p^{n-2}a, \cdots, pa$，$a$ 依次地添加到已经作出的子群上.

设 λ 是组成陪集 $X+a$ 的元素的型中最大的；这样的一个最大型是存在的，因为陪集 $X+a$ 只含有限多个元素. 其次，设 $a'=x_0+a$ 是陪集 $X+a$ 中一切 λ 型元素在子群 A^λ 中高度最大的元素之一. 如果元素 a' 在 A^λ 中的高度是 $n-1$ 且 $a'=p^{n-1}\bar{a}$，其它 $\bar{a}\in A^\lambda$，那末令

$$\overline{X}=\{X, \bar{a}\}.$$

子群 $\overline{X}$ 是有限的并且既包含子群 X 又包含元素 $a=a'-x_0$. 我们证明，$\overline{X}$ 是群 A 的完全子群.

子群 $\overline{X}$ 中任意元素都有(因为 $p^n\bar{a}\in X$) $\bar{x}=x+k\bar{a}$ 的形式，此处 $x\in X$，$0\leqslant k<p^n$. 如果元素 $\bar{x}$ 的型为 α 且 $\bar{x}$ 在 A^α 中的高度为 s，因而

$$\bar{x}=x+k\bar{a}=p^s c, \quad c\in A^\alpha, \tag{1}$$

那末元素 $A^{\alpha+1}+\bar{x}$ 在商群 $\frac{A^\alpha}{A^{\alpha+1}}=\overline{A}^\alpha$ 中的高度也等于 s(利用子群 $A^{\alpha+1}$ 的定义!). 我们要证明，在子群 $\overline{X}$ 中可以找到这样一个 α 型元素 $\bar{x}'$，使得

$$p^s(A^{\alpha+1}+\bar{x}')=A^{\alpha+1}+\bar{x}.$$

当 $k=0$ 且 $\alpha<\lambda$ 时，$k\bar{a}\in A^{\alpha+1}$. 在这两个情形下，我们的论断可由子群 X 在 A 中的完全性推出. 其次，如果 $\alpha=\lambda$ 并且 k 能被 p^s 整除，$k=p^s k'$，那末根据(1)，将有 $x=p^s(c-k'\bar{a})$. 由 $c-k'\bar{a}\in A^\lambda$ 以及子群 X 的完全性可以推出，在子群 $A^\lambda\cap X$ 中存在这样的元素 x'，使得

$$A^{\lambda+1}+x=p^s(A^{\lambda+1}+x'),$$

由此得出

$$A^{\lambda+1}+\bar{x}=p^s(A^{\lambda+1}+x'+k'\bar{a}),$$

并且显然 $x'+k'\bar{a}\in(A^\lambda\cap\bar{X})$.

我们证明，在所有其他情形，等式(1)与元素 a' 的选法相矛盾.

设 p^j 是可以整除 k 的数 p 的最高幂，$k=p^jk'$；因为 $k<p^n$，所以 $j\leqslant n-1$. 由于数 k' 与 p 互素，因此存在这样的整数 m 与 l，$0<l<p$，使得 $k'l=1+mp$. 将等式(1)的两边同时乘以 lp^{n-j-1} 就得出

$$lp^{n-j-1}x+p^{n-1}\bar{a}+p^nm\bar{a}=p^{n+s-j-1}(lc),$$

而由于 $p^n\bar{a}\in X$ 得出

$$lp^{n-j-1}x+p^nm\bar{a}=x'\in X,$$

由此，因为 $p^{n-1}\bar{a}=a'$ 及 $lc=c'\in A^\alpha$，可知

$$x'+a'=p^{n+s-j-1}c'.$$

如果 $\alpha>\lambda$，那末由 $x'+a'\in A^\alpha$ 推出，在陪集 $X+a'=X+a$ 中可以找出一个型大于 λ 的元素，这就与加在元素 a' 上的条件相矛盾. 如果 $\alpha=\lambda$，但 k 不能被 p^s 整除，那末 $j\leqslant s-1$，由此得出 $n+s-j-1\geqslant n$. 因此，在陪集 $X+a$ 中我们找到一个 λ 型的元素，它在 A^λ 中的高度大于元素 a' 的高度 $n-1$，这又和元素 a' 的选择相矛盾. 子群 $\bar{X}$ 的完全性就此证明.

我们知道，元素 $p^n\bar{a}$ 包含在子群 X 内，而且这个元素的型不小于 λ. 由于 X 是一个完全子群，在它里面可以找到一个或者型为 λ 或者等于零元的元素 x_1 以及一个型不小于 $\lambda+1$ 的元素 x_2，使得

$$p^n\bar{a}=p^nx_1+x_2.$$

如果 $\bar{a}-x_1=\bar{\bar{a}}$，那末

$$p^n\bar{\bar{a}}=x_2,\ x_2\in A^{\lambda+1}, \tag{2}$$

于是仍有 $\bar{X}=\{X,\bar{a}\}$. 所有元素 $k\bar{a}$, $0<k<p^n$, 都不包含在子群 X 内. 其次，我们知道，$\bar{X}$ 中所有不属于X的元素的型都不会超过 λ——这一点可以由刚才所证明的当 $k\neq 0$ 和 $\alpha>\lambda$ 时等式(1)的不可能性推出. 由此推出，群 $\bar{A}^{\lambda}_{\bar{X}}$ 是子群 $\bar{A}^{\lambda}_{X}$ 与元素 $\bar{a}+A^{\lambda+1}$ 在群$\bar{A}^{\lambda}$ 中所生成的 p^n 阶循环群的直和. 由于子群 $\bar{X}$ 的完全性，所以有限子群 $\bar{A}^{\lambda}_{\bar{X}}$ 是 Ulm 因子 $\bar{A}^{\lambda}$ 中的纯子群，因而，根据 § 25 中的结果，是群 $\bar{A}^{\lambda}$ 的一个直被加群. 子群 $\bar{A}^{\lambda}_{X}$ 同样也是 $\bar{A}^{\lambda}$ 的直被加群，同时我们还证明了在群 $\bar{A}^{\lambda}$ 中存在一个 p^n 阶循环直被加群，它与 $\bar{A}^{\lambda}_{X}$ 的交是 0.

现在让我们转来考察群 B. 由于在同构 φ 之下子群X与Y中的元素的型被保持，所以群 $\bar{A}^{\lambda}_{X}$ 与 $\bar{B}^{\lambda}_{Y}$ 同构. 子群 $\bar{B}^{\lambda}_{Y}$ 既然是群 $\bar{B}^{\lambda}$ 中的一个有限纯子群，它应该是这个群的一个直被加群，但因为根据 Prüfer 第二定理，$\bar{B}^{\lambda}$ 可以分解成为循环群的直和，并且根据 Ulm 定理的条件，它与群 $\bar{A}^{\lambda}$ 同构，所以在 $\bar{B}^{\lambda}$ 中可以找到一个 p^n 阶循环直被加群，它与子群 $\bar{B}^{\lambda}_{Y}$ 的交是 0. 设这个循环群的生成元(即以 $B^{\lambda+1}$ 为模的陪集)是 $b+B^{\lambda+1}$. 元素 b 在群B中有型 λ，并且 $p^nb\in B^{\lambda+1}$. 如果在同构 φ 之下，元素 y_2 与元素 x_2 相对应，那末 $y_2\in B^{\lambda+1}$，而在 B^{λ} 中存在这样的一个元素 b_0，使得 $p^{n-1}b_0=y_2-p^nb$. 我们现在引入记号 $\bar{b}=b+pb_0$，因而

$$p^n\bar{b}=y_2, \tag{3}$$

并且令

$$\bar{Y}=\{Y,\bar{b}\}.$$

我们注意，$p^{n-1}\bar{b}\notin Y$. 事实上，由 $p^{n-1}\bar{b}=y_0$, $y_0\in Y$ 将推出

$$y_0-p^{n-1}b=p^nb_0.$$

但是，当我们过渡到因子 $\bar{B}^{\lambda}$ 时，这将导致在直被加群 $\bar{B}^{\lambda}_{Y}+\{B^{\lambda+1}+b\}$ 中存在这样一个元素，它在 $\bar{B}^{\lambda}$ 中的高度大于它在直被加群 $\{B^{\lambda+1}+b\}$ 中的分支的高度，这是不可能的. 由此也推出，在群 $\bar{B}^{\lambda}$

中，子群 $\bar{B}_Y^\lambda$ 与$\{B^{\lambda+1}+\bar{b}\}$构成一个直和.

由 $p^{n-1}b\notin Y$ 及等式(2)和(3)以及元素 x_2 和 y_2 在同构 φ 之下彼此对应推出，子群 $\bar{X}$ 与 $\bar{Y}$ 同构：在同构 φ 之下把子群 $\bar{X}$ 映到子群 $\bar{Y}$ 上而使元素 $\bar{b}$ 与元素 $\bar{a}$ 对应，我们就得到这两个子群之间的一个同构 $\bar{\varphi}$. 同构 $\bar{\varphi}$ 是同构 φ 的延拓. 这个同构同时还保持元素的型. 事实上，如果元素 $\bar{x}=x+k\bar{a}$ 与 $\bar{y}=y+k\bar{b}(0\leqslant k<p^n)$ 在同构 $\bar{\varphi}$ 之下彼此对应，那末由于 $x\varphi=y$，元素 x 与 y 的型相同. 因此，当 $k=0$ 时这一论断对元素 $\bar{x}$ 与 $\bar{y}$ 来说也正确. 如果 $k\neq 0$，但元素 x 与 y 的型不等于 λ，那末元素 $\bar{x}$ 与 $\bar{y}$ 的型仍旧相同，因为元素 $k\bar{a}$ 与 $k\bar{b}$ 的型为 λ，而两个不同型的元素的和的型显然等于这两个型中较小的那一个. 最后，如果 $k\neq 0$ 且元素 x 与 y 的型为 λ，那末元素 $\bar{x}$ 与 $\bar{y}$ 的型也是 λ，因为在群 $\bar{A}^\lambda$ 中(相应地在群 $\bar{B}^\lambda$ 中)子群 $\bar{A}_X^\lambda$ 与$\{A^{\lambda+1}+\bar{a}\}$(相应地，$\bar{B}_Y^\lambda$ 与$\{B^{\lambda+1}+\bar{b}\}$)构成直和.

现在剩下要我们证明的是，子群 $\bar{Y}$ 是群 B 中的完全子群. 只要将上面证明 $\bar{X}$ 是 A 中的完全子群时所作的论证重复一遍，而把那里的元素 $\bar{a}$ 现在取为元素 $\bar{b}$，那里的元素 a' 现在取为元素 $p^{n-1}\cdot\bar{b}$，就可以证明这一点. 事实上，元素 $\bar{b}$ 在子群 B^λ 中的高度为零，其次，陪集 $Y+p^{n-1}\bar{b}$中所有元素的型不大于元素$p^{n-1}\bar{b}$ 的型 λ，最后，如果在这一陪集中可以找到一个 λ 型元素，它在群B^λ中的高度大于 $n-1$，那末我们就会得出和子群 $\bar{B}_Y^\lambda+\{B^{\lambda+1}+\bar{b}\}$是群 $\bar{B}^\lambda$的直被加群这一事实相矛盾的结论. 预备定理证毕.

现在证明 Ulm 定理已经没有任何困难了. 我们利用自然数各把群 A 与 B 的所有元素编上号. 然后在这两个群中选取子群 $X_0=0$ 及 $Y_0=0$. 假设对于所有 k, $0\leqslant k<n$，已经找出满足预备定理中全部条件的子群 $X_k\subset A$ 及 $Y_k\subset B$，且存在于子群 X_k 与 $Y_k(k=0,1,\cdots,n-1)$ 之间的同构 φ_k 各为其前一个的延拓. 现在可以根据预备定理来构成子群 X_n 及 Y_n，并且当 n 为奇数时，

取群A中不属于X_{n-1}的元素中标数最小的元素作为a，而当n为偶数时在群B中取类似的元素．我们得出，群A是递增子群列

$$A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_n \subset \cdots$$

的并集，而群B是递增子群列

$$B_0 \subset B_1 \subset B_2 \subset \cdots \subset B_n \subset \cdots$$

的并集，并且在子群A_n与B_n，$(n=0,1,2,\cdots)$之间存在着同构φ_n，它是同构φ_{n-1}的延拓．由此推出，群A与B同构．Ulm 定理被证明．

利用 Ulm 定理和前一节的存在定理，可以证明以下的定理（参看 Baer[15]），这个定理对于群的直积的一般理论来说也是有意义的．

若群G是一个可数既约准素群，那末这个群的任意两个直分解都具有同构延拓的充分与必要条件是，这个群的型等于 1.

事实上，如果$\tau=1$，那末根据 Prüfer 第二定理，群G可以分解成为循环群的直和，然后再应用§24中的结果．另一方面，设$\tau>1$并且设 Ulm 因子$\overline{G}^{\sigma}$，$0\leqslant\sigma<\tau$，已被分解成阶为

$$p^{n_{\sigma,1}}, p^{n_{\sigma,2}}, \cdots, p^{n_{\sigma,k}}, \cdots$$

的循环群的直和，此处$n_{\sigma,1}<n_{\sigma,2}<\cdots<n_{\sigma,k}<\cdots$[1]．令$\overline{G}^{\sigma}=A_{\sigma}+B_{\sigma}$，此处$A_{\sigma}$是群$\overline{G}^{\sigma}$的这一分解中对奇数$k$的一切$p^{n_{\sigma,k}}$阶循环被加群的直和，$B_{\sigma}$是同样的直和，但$k$取偶数．于是存在群$A$及$B$，它们的 Ulm 因子列分别是序列$A_0, A_1, \cdots, A_{\sigma}, \cdots$及$B_0, B_1, \cdots, B_{\sigma}, \cdots$．直和$A+B$的 Ulm 因子与群$G$的 Ulm 因子一致，因此，根据 Ulm 定理，

$$G \simeq A+B.$$

另一方面，存在群$\overline{A}$及$\overline{B}$，它们的 Ulm 因子列分别是$B_0, A_1, \cdots,$

---

1) 这自然不是说，在群$\overline{G}^{\sigma}$的分解中，只出现一个阶$p^{n_{\sigma,k}}$的循环被加群．

$A_\sigma, \cdots$及 $A_0, B_1, \cdots, B_\sigma, \cdots$，并且同样有

$$G \simeq \bar{A} + \bar{B}.$$

由上一节所证明的关于直和的 Ulm 因子等于它的直被加群的 Ulm 因子的直和这一定理容易推出，我们所作的群G的这两个直分解没有同构的延拓.

关于在什么条件下，一个不可数的既约准素群的任意两个直分解具有同构延拓的问题迄今尚未解决，甚至连条件 $\tau=1$ 是不是一个必要条件或充分条件，也还不知道. 关于这一方面我们举出 Куликов[2]的一个结果，但不加以证明：如果准素群G是某一循环群直和的闭包(在 § 26 意义下)，那末它的任意两个直分解都具有同构延拓.

在结束本节时，我们还要讨论一下 Ulm 定理是否能推广到不可数情形的问题. 到目前为止，还没有证明过任何关于把具任意势的既约准素群的研究归结为不含无限高度元素准素群的研究，而且在可数情形下就变成 Ulm 定理的那种定理. 无论如何，只是单纯地由 Ulm 定理的陈述中去掉"可数"一词而得出来的这样的定理，是不能被证明的—— Куликов[2]曾找到一些反例. 在这些例子里所指出的群都具有可数型. 下面叙述的是一个型为 2 的既约准素群的例子；这个例子是 Л. Я. Куликов 告诉作者的并且在这里初次发表.

Куликов 的例子. 用 $Z_i(i=1,2,\cdots)$表示 p^i 阶循环群，A 表示这些循环群直和的闭包(参看 § 26). 这样，A 就是由每一个 Z_i 中取出一个元素作成的序列所构成的群，并且在每一个这样的序列中，所有元素的阶全体有界. 令B是群A中一切只有有限个非零分支的 p 阶元素所组成的子群，C 是一切这样的 p 阶元素所组成的子群，这些元素只有有限个标号为奇数的非零分支，而同时标号为偶数的分支则不受任何限制. 很明显，

$$B \subset C \subset A_1,$$

这里 A_1 是群 A 的底层.

我们证明以下的论断.

群 $H=\frac{A}{B}$ 与 $G=\frac{A}{C}$ 是互不同构的既约准素群，它们的型都是 2 并且它们的Ulm因子同构.

我们令 $H^*=\frac{A_1}{B}$ 并来证明，H^* 是由群 H 中具有无限高度的元素所组成的. H^* 中任意元素 h^* 都有 $h^*=a+B$ 的形式，此处 a 是 A 中的一个 p 阶元素，元素 a 的第 i 个分支用 z_i 来表示. 如果数 n 已取定，那末对于任意 $i>n$，在群 Z_i 中都存在这样的元素 z_i'，使得 $p^n z_i'=z_i$. 其次，在 $i \leqslant n$ 时令 $z_i'=0$. 于是

$$z'=(z_1', z_2', \cdots, z_i', \cdots)$$

是群 A 中的一个 p^{n+1} 阶元素，并且 $p^n z'-a \in B$，即 $p^n(z'+B)=h^*$. 这就证明了，元素 h^* 在群 H 中有无限高度，即

$$H^* \subset H^1, \tag{4}$$

这里 H^1 是群 H 的无限高度元素所作成的子群.

其次，由 $H=\frac{A}{B}$, $H^*=\frac{A_1}{B}$ 得出同构关系

$$\frac{H}{H^*} \simeq \frac{A}{A_1}.$$

但是，因为映射 $a \to pa$, $a \in A$，是群 A 到子群 pA 上的同态映射，它的核为 A_1，所以 $\frac{A}{A_1} \simeq pA$. 因此

$$\frac{H}{H^*} \simeq pA. \tag{5}$$

因为群 pA，和群 A 本身一样，不含无限高度元素，所以由(4)及(5)推出

$$H^1 \simeq H^*, \tag{6}$$

$$\frac{H}{H^1} \simeq pA. \tag{7}$$

我们已经求出了群H的 Ulm 因子并且特别地，证明了群H是一个型为 2 的既约群.

现在我们来找出群G的 Ulm 因子. 如果令 $D=\frac{C}{B}$, 那末由于 $G=\frac{A}{C}$, $H=\frac{A}{B}$将有

$$G \simeq \frac{H}{D}. \tag{8}$$

由 $D \subset H^*$ 及(6)推出 $D \subset H^1$，因而由(8)推出

$$G^1 \simeq \frac{H^1}{D}, \tag{9}$$

此处 G^1 是群G中具无限高度元素的子群：如果元素 $h+D$ 在群 $\frac{H}{D}$中有无限高度，那末对于任意 n，存在这样的元素 $h_n \in H$ 和 $d_n \in D$，使得 $p^n h_n = h + d_n$；但是元素 d_n 在群H中具有无限高度，因此元素 h 的高度也是无限的.

由(8)与(9)推出

$$\frac{G}{G^1} \simeq \frac{H}{H^1}. \tag{10}$$

另一方面，根据(6)，群 H^1 具连续统的势并且由 p 阶元素所构成. 这一点对于群 G^1 来说也是正确的：由(9)，(6)及群 H^* 与 D 的定义推得，

$$G^1 \simeq \frac{A_1}{C},$$

但商群$\frac{A_1}{C}$由 p 阶元素组成并且具连续统的势. 应用 Prüfer 第一定理(§24)，我们得出同构关系

$$G^1 \simeq H^1. \tag{11}$$

这就证明了，群 G 是一个型为 2 的既约群，它的 Ulm 因子分别与群 H 的 Ulm 因子同构.

还要证明群 H 与群 G 不同构. 为此，注意到包含关系 $H^1\subset H_1$, $G^1\subset G_1$，此处 H_1 与 G_1 分别是群 H 与 G 的底层，就只要证明商群 $\frac{H_1}{H^1}$ 与 $\frac{G_1}{G^1}$ 具有不同的势即可.

由(6)我们知道，$H^1=\frac{A_1}{B}$. 另一方面，容易看出，$H_1=\frac{L}{B}$，此处 L 表示群 A 中一切 p 阶元素和一切只有有限个异于零的 p^2 阶分支的 p^2 阶元素所构成的子群. 由此推出，

$$\frac{H_1}{H^1}\simeq\frac{L}{A_1};$$

但商群 $\frac{L}{A_1}$ 是一个可数群.

现在让我们考察商群 $\frac{G_1}{G^1}$. 首先，

$$G^1=\frac{A_1}{C}. \tag{12}$$

事实上，因为 $D\subset H^1$，所以在群 H 到群 $G\simeq\frac{H}{D}$ 的自然同态之下，子群 G^1 的完全原象就是子群 H^1. 但由(6)可知，A_1 是子群 H^1 在群 A 到群 $H=\frac{A}{B}$ 上的自然同态之下的完全原象. 由此推出，在群 A 到群 $G=\frac{A}{C}$ 的自然同态之下，子群 G^1 的完全原象就是子群 A_1；这就证明了等式(12).

另一方面，$G_1=\frac{K}{C}$，这里 K 表示群 A 中由一切 p 阶元素以及一切这样的 p^2 阶元素所组成的子群，这些 p^2 阶元素只有有限多个标号为奇数的 p^2 阶分支，而标号为偶数的 p^2 阶分支则可能有无

限多个. 由此及(12)推知,

$$\frac{G_1}{G^1}\simeq\frac{K}{A_1};$$

但是商群$\frac{K}{A_1}$具有连续统的势.

这就证明了群H与G不同构[参看补充 30.3.]

§29. 混合阿贝尔群

混合阿贝尔群G叫做分枝的，假如它可以分解为一个周期群及一个无扭群的直和. 显然，周期被加群与群G的周期部分F重合,而无扭被加群与商群$\frac{G}{F}$同构.

一切循环群的直和,特别，一切具有限生成系的阿贝尔群,以及一切完备群都是分枝群. 但是，下面就会看到，并不是所有混合群都是分枝的. 由于这一点，关于可分枝的条件问题，也就是说,在什么条件下,混合群的研究可以归结为周期群和无扭群的研究的问题,就成合混合群理论中的基本问题.

我们证明以下定理，同时在证明过程中将要作出几个非分枝群的例子.

凡周期部分与一个给定的周期群F同构的任何一个阿贝尔群是分枝群的充分必要条件是，群F可分解成为一个完备群和元素的阶全体有界的一个群的直和.

下面关于定理中条件的充分性的简单证明是 Куликов[1]指出的. 设$F=F_1+F_2$,其中F_1是完备群,F_2的元素的阶全体有界,又设F是阿贝尔群G的周期部分. 如在§23 中所证,完备子群F_1可以作为一个直被加群从群G中分出来,

$$G=F_1+G'.$$

这时群G'的周期部分F'与群F_2同构,这就是说，它的元素的阶

全体有界，但因为子群 F' 是群 G' 的纯子群，所以，如在§25中所证，它是 G' 的一个直被加群. 这就证明了群 G 是一个分枝群.

我们转来证明定理中条件的必要性. 首先证明以下预备定理.

若周期群 F 可以分解成两个群的直和，$F=F'+F''$，并且存在一个非分枝群 G，以 F'' 为其周期部分，那末周期部分与 F 重合的群 $H=F'+G$ 也是一个非分枝群.

事实上，如果存在分解

$$H=F+H_0=F'+F''+H_0,$$

其中 H_0 是一个无扭群，那末与群 G 同构的商群 $\frac{H}{F'}$ 也是一个分枝群.

这个预备定理使得我们以下可以限于讨论群 F 是既约的情形. 如果在这一假定之下，群 F 的元素的阶不全体有界，那末下面两种可能一定有一个成立：或者在把群 F 分解成准素群直和时，在这些准素直被加群中的某些个的元素不全体有界，或者这些直被加群的个数无限. 我们分别考察这两种情形.

在第一种情形下，根据预备定理，可以假定群 F 本身是准素的. 这样，给定的是一个包含具任意大阶数的既约准素群 F（对一个素数 p 的）. 我们用 $F_k(k=1, 2, \cdots)$ 来表示群 F 中一切在 F 内高度不小于 k 的元素所组成的子群. 其次，在 F 中选取元素组 $a_1, a_2, \cdots, a_i, \cdots$ 及 $b_1, b_2, \cdots, b_i, \cdots$，它们具有以下性质（都是对 $i=1, 2, \cdots$ 而言）：1) $b_{i+1}=b_i+p^i a_{i+1}$，$b_1=a_1$；2) 元素 b_i 的阶随着 i 无限制地增大；3) 在元素 b_i 所在的对子群 F_i 的陪集中，以 b_i 的阶最小. 这两组元素可以按以下方式作出：在对子群 F_1 的一个陪集中（但不在 F_1 内）选取一个具最小阶的元素作为 b_1，并且令 $a_1=b_1$. 假设元素 b_i 与 a_i 已经选出并且设元素 b_i 的阶是 p^s. 由于群 F 中元素的阶无界以及由于这个群的既约性使得我们可以在它里

面找到一个非零元素 x，它的高度 k 是有限的并且大于 $s+i$. 其次，设元素 y 满足等式 $p^k y=x$. 我们选取元素 $b_i+p^i y$ 所在的对子群 F_{i+1} 的陪集中的一个阶数最小的元素并且把它记作 b_{i+1}. 如果

$$b_{i+1}=b_i+p^i y+p^{i+1}f, f\in F,$$

那末就令 $a_{i+1}=y+pf$, 由此推出 $b_{i+1}=b_i+p^i a_{i+1}$. 还剩下证明，元素 b_{i+1} 的阶大于元素 b_i 的阶. 事实上，由 $p^s b_{i+1}=0$ 将得出 $p^{s+i}y+p^{s+i+1}f=0$, 由此，因为 $s+i<k$,

$$p^k y=x=p^{k+1}(-f),$$

但是这与元素 x 的高度是 k 这一事实矛盾.

现在我们要作出一个阿贝尔群 G. 这个群的生成系由群 F 中所有元素以及可数多个元素 $v_1, v_2, \cdots, v_i, \cdots$ 组成，而它的定义关系则是交换性关系，群 F 中元素间的所有关系，最后，还有关系

$$pv_{i+1}=v_i+a_i,\quad i=1,2,\cdots \tag{1}$$

在这里 a_i 是按照上面所述的方式定义的元素. 由关系(1)所推出的任何一个结果都可以写成

$$\sum_{i=1}^{n} k_i(pv_{i+1}-v_i-a_i)=0 \tag{2}$$

的形式，此处 $n\geqslant 1$, k_i 是整数且 $k_n\neq 0$. 但是在关系(2)中元素 v_{n+1} 的系数不为零，因而由关系(1)不可能推出在 F 中不为零的某些 F 的元素等于零的结果. 换句话说，群 F 是群 G 的子群. 其次，我们还得出，由关系(1)不可能推出关系 $kv_1=a$, 此处 $k\neq 0$, $a\in F$, 也就是说，元素 v_1 的阶是无限的. 因此，商群 $\frac{G}{F}$ 是无扭群[1)]，而 F 是群 G 的最大周期子群.

1)　容易看出，它与 p 进分数群 R_p 同构.

现在假定F是G的直被加群，即$G=F+H$. 于是$v_i=f_i+h_i$, $f_i\subset F, h_i\subset H, i=1,2,\cdots$. 因为$a_i\in F$，所以由关系(1)可以推出

$$pf_{i+1}=f_i+a_i.$$

特别，$pf_2=f_1+a_1=f_1+b$. 假定已经证明了

$$p^{i-1}f_i=f_1+b_{i-1},$$

那末

$$p^if_{i+1}=p^{i-1}f_i+p^{i-1}a_i=f_1+b_{i-1}+p^{i-1}a_i=f_1+b_i,$$

而因为$p^if_{i+1}\in F_i$，所以我们得出，当$i=1,2,\cdots$时，元素f_1与b_i属于对子群F_i的同一个陪集. 由此，根据元素b_i的定义得出，元素f_1的阶不小于元素b_i的阶，但是元素b_i的阶随着i无限增大，于是就导致与元素f_1的阶的有限性相矛盾的结果. 这样就证明了，*F不是G的直被加群.*

我们现在转来考察上面所指出的第二个情形. 也就是说，假定*群F是无限多个对于不同的素数$p_1, p_2, \cdots, p_i, \cdots$的既约准素群的直和，*

$$F=\sum_i F_{p_i}. \tag{3}$$

在子群F_{p_i}的每一个里我们选出一个高度为0的非零元素a_i并且按下述方式构成阿贝尔群G：它的生成元是群F中所有元素，此外再加元素$v_0, v_1, \cdots, v_i, \cdots$，而它的定义关系是交换性关系，群$F$中元素间的所有关系，最后还有关系

$$p_iv_i=v_0+a_i, i=1,2,\cdots. \tag{4}$$

如同前一情形一样，容易看出，F是群G的子群，并且是它的最大周期子群.

假定F是G的直被加群，即$G=F+H$. 那末$v_i=f_i+h_i$, $f_i\in F, h_i\in H, i=0,1,2,\cdots$. 因为$a_i\in F$，所以由关系(4)推出

$$p_if_i=f_0+a_i, \quad i=1,2,\cdots \tag{5}$$

元素 f_0 是从分解(3)的直被加群中所取出的有限个分支的和，因此可以找出这样的一个标数 j，使得元素 f_0 在 F_{p_j} 中的分支等于零．如果把元素 f_j 在直被加群 F_{p_j} 中的分支记作 f'_j，那末等式(5)在 $i=j$ 时就变成等式

$$p_j f'_j = a_j,$$

但是这与元素 a_j 在群 F_{p_j} 中的高度是零这一事实相矛盾．

这就结束了定理的证明．

混合群 G 可分枝的条件也可以用它的周期部分 F 和商群 $\frac{G}{F}$ 的性质之间的关系的形式给出来．Baer[3]就是这样来研究这个问题的，但他对无扭群 $\frac{G}{F}$ 加上一些限制，不过，假如这个群是可数的话，这些限制自然总能满足．上面所证明的定理实际上是 Baer 的结果的推论．对于这个问题的另外的处理，是同混合群的自同构关联着的，包含在 Мишина 的论文[2]中．在 Ляпин 的论文[3]中也可以找到可分枝性的一个判断法．至于一个无扭群 H 应该满足什么样的条件，才能使任何一个阿贝尔群(在它对其周期部分的商群是 H 时)的商群是分枝的，这样的条件到目前为止还没有建立起来．[参看补充 32.]

不要把混合群的分枝问题和混合群的分解问题混为一谈．前面作出了非分枝的混合阿贝尔群的例子．但是任何一个混合阿贝尔群 G 都可以分解成为直和(Куликов[1])．

事实上，如果群 G 的周期部分 F 是完备的，那末 F 是 G 的直被加群．如果 F 不是完备的，那末利用 §25 的结果，包括本节的预备定理，在 F 中可以找到一个循环直被加群 A．子群 A 既然是 F 的纯子群，它也是群 G 的纯子群，而因为这个子群又是一个有限群，这也就是说，它的元素的阶全体有界，所以再根据 §25，A 可以作为一个直被加群从 G 中分出来．

第八章　无扭阿贝尔群

§30. 秩是1的群·无扭群元素的型

无扭阿贝尔群的研究到目前为止比较起来，例如比起准素阿贝尔群来要少得多. 在无扭阿贝尔群的理论中要大用群的秩这一概念(参看§19)，并且有限秩的群将作为一个基本研究对象而出现. 在无扭阿贝尔群理论的各种著作中称之谓自足子群，闭子群，除子群等等的纯子群(参看§25)这个概念也在这里占有极重要的地位.

应该考虑到这一事实，在无扭阿贝尔群里，方程

$$nx=a,\ n>0 \tag{1}$$

的解不多于一个，因为它的两个解的差将是有限阶元素. 由此推出，无扭阿贝尔群G的子群C是纯子群，当且仅当商群$\dfrac{G}{C}$是无扭群. 由方程(1)的解的唯一性还可以推出，无扭阿贝尔群G的任意一组纯子群的交仍是这个群的纯子群. 因此，我们可以谈论由群G的一些元素的集合M所生成的群G的纯子群，把它就理解为群G中一切含M的纯子群的交；这样的子群显然是存在的，G本身就是其中的一个.

无扭群G的由集合M所生成的纯子群由G中一切与集合M线性相关(在§19的意义下)的元素所组成.

事实上，如果元素a与集合M线性相关，这就是说，如果元素a的某一倍数在子群$\{M\}$内，那末这个倍数也在M所生成的纯子群内，因为后者显然包含子群$\{M\}$，因而元素a本身也在M所生成的纯子群内. 另一方面，群G的一切与集合M线性相关的元素构

成一个子群：任意两个元素，如果它们的某一倍数属于$\{M\}$，那末它们的和与差也具有这一性质．这个子群包含M并且是G中的纯子群：若$nb=a$且$ka\in\{M\}$，那末$(kn)b\in\{M\}$，即b与M线性相关．

由§23我们知道，任何一个阿贝尔群都包含在某一完备阿贝尔群内．我们甚至可以断言，任何一个无扭阿贝尔群都包含在某一完备无扭阿贝尔群内，即包含在若干R型群的直和内．这一点不难由§23中所引入的相应定理的证明推出，但是也可以直接证明这一论断：如果无扭群G包含在一个混合完备群H内，那末群G与群H的周期部分的交等于零，因此群G同构地映入群H对其周期部分的商群内，而这个商群是一个完备无扭群．

任何一个具有限秩n的无扭阿贝尔群G都包含在一个秩n的完备无扭阿贝尔群内，即包含在n个R型群的直和内．

事实上，群G包含在某一个完备无扭群H内．它所生成的群H的纯子群$\bar{G}$也是完备的．而前面已经证明，$\bar{G}$的任意一个元素都与G线性相关，因而与群G的任意一个极大线性无关系线性相关．因此，群$\bar{G}$的秩等于n．

特别地，由此推出，任何一个秩1的无扭群都与有理数加法群R的一个子群同构．这样，当我们得到所有秩1的无扭阿贝尔群的完全描述时（这是这一节的目的），那末同时就得到了群R的所有子群精确到同构的描述．

我们引入一个辅助概念．我们称任意形式如

$$\alpha=(\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots)$$

的序列为一个特征，此处每一个α_n或者是零，或者是自然数或者是符号∞．特征α与

$$\beta=(\beta_1, \beta_2, \cdots, \beta_n, \cdots)$$

说是等价的，假如除去可能的有限多个都异于∞的α_n与β_n外，对

于一切 n 来说，都有 $\alpha_n=\beta_n$. 显然，所有特征可分成互不相交的等价特征类；这些类叫做型[1]，并且用字母 $\mathfrak{a},\mathfrak{b},\mathfrak{c},\cdots$来表示.

在型的集合中如下地引入一个偏序关系：$\mathfrak{a}\leqslant\mathfrak{b}$，假如型 $\mathfrak{a}$ 里存在这样的特征 α 而型 $\mathfrak{b}$ 里存在这样的特征 β，使得对一切 n 来说，$\alpha_n\leqslant\beta_n$；自然，这时符号∞被认为大于任何自然数. 利用型的定义，读者不难验证以下的论断是正确的：

1) $\mathfrak{a}\leqslant\mathfrak{a}$;

2) 若 $\mathfrak{a}\leqslant\mathfrak{b}$, $\mathfrak{b}\leqslant\mathfrak{c}$, 那末 $\mathfrak{a}\leqslant\mathfrak{c}$;

3) 若 $\mathfrak{a}\leqslant\mathfrak{b}$, $\mathfrak{b}\leqslant\mathfrak{a}$, 那末 $\mathfrak{a}=\mathfrak{b}$，即两个型重合.

一切型中最大的是由唯一的特征

$$(\infty,\infty,\cdots,\infty,\cdots)$$

所组成的型；这个型由于下面就会明白的原因，我们把它叫做 R 型. 一切型中最小的是由特征

$$(0,0,\cdots,0,\cdots)$$

所组成的型，这个型我们称作零型.

设给定了型 $\mathfrak{a}$ 及 $\mathfrak{b}$. 我们在它们里面分别选取特征 α 及 β 并且引入记号

$$\gamma_n=\min(\alpha_n,\beta_n),\ n=1,2,\cdots.$$

容易看出，由特征

$$(\gamma_1,\gamma_2,\cdots,\gamma_n,\cdots)$$

所确定的型 $\mathfrak{c}$ 与在型 $\mathfrak{a}$ 及 $\mathfrak{b}$ 中的特征 α 及 β 的选取无关. 这个型是一切小于或等于型 $\mathfrak{a}$ 及型 $\mathfrak{b}$ 的型中最大的；型 $\mathfrak{c}$ 叫做型 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的积，$\mathfrak{c}=\mathfrak{a}\mathfrak{b}$. 显然，类似地可以谈论任意有限个型的积[2].

我们转来描述**秩1的无扭阿贝尔群**. 令 $p_1,p_2,\cdots,p_n,\cdots$是所

1) 也叫做族.

2) 我们也可以证明，在大于或等于型 $\mathfrak{a}$ 及 $\mathfrak{b}$ 的型中有一个最小的. 换一句话说，型的集合是一个格(参看§43).

有素数的序列，它们是按照递增的顺序来编号的．其次，令G是秩1的无扭阿贝尔群而a是G中一个不等于零的元素．我们使特征α与群G对应，如果方程$p_n x=a$在G中没有解，那末就令$\alpha_n=0$，如果方程$p_n^k x=a$在G中可解，但方程$p_n^{k+1}x=a$在G中不可解，那末就令$\alpha_n=k$，如果一切方程$p_n^i x=a$，$i=1,2,\cdots$在G中都有解，那末就令$\alpha_n=\infty$．容易证明，把元素a换成元素ma后，此处m是一个不为零的整数，如果符号α_n是∞，那末α_n不改变，如果α_n是有限的并且等于$k\geqslant 0$，而$m=p_n^l m'$，$(p_n, m')=1$，那末经过代替后，将有$\alpha_n=k+l$；换句话说，在这种情况下，特征又被与它等价的特征所代替．如果把元素a用G中任意一个不为零的元素b来代替，这一事实也成立，因为元素a与b具有异于零的公倍数．反过来，如果特征β与特征α等价，那末可以找到这样一个元素b来代替元素a，借助于这个元素，特征β与群G对应．事实上，若$\alpha_n-\beta_n=\mu_n>0(n=i_1, i_2, \cdots, i_s)$与$\beta_n-\alpha_n=\nu_n>0(n=j_1, j_2, \cdots, j_t)$，而对于所有其余的$n$，$\alpha_n=\beta_n$，那末就取方程

$$p_{i_1}^{\mu_1}p_{i_2}^{\mu_2}\cdots p_{i_s}^{\mu_s}x=p_{j_1}^{\nu_1}p_{j_2}^{\nu_2}\cdots p_{j_t}^{\nu_t}a$$

的解作为b；容易看出，这个解在G中是存在的．

我们得到，对于任意一个秩1的无扭阿贝尔群，都有一个唯一确定的型与它对应．互不同构的群有不同的型与它们对应．事实上，如果借助于元素a，特征α与群G对应，那末对于任意一个使$a_n<\infty$的n来说，方程$mx=a$在G中有解，当且仅当m能被p_n的不大于α_n次幂所整除——如果元素b与c满足等式$pb=a$与$qc=a$，其中p与q是互素的数，那末方程$(pq)x=a$被元素$tb+sc$所满足，此处$ps+qt=1$．这样，在把群G映入有理数加法群R，而元素a映成数1的映射之下，群G被映到群R的子群R_α上，这个子群由一切这样的有理数所组成，它们的分母(在既约写法之下)能被素数p_n的不大于α_n次幂所整除，假如$\alpha_n<\infty$；而能被p_n的

任意次幂所整除，假如$\alpha_n=\infty$. 但是R_α是R中包含整数且具有下述性质的唯一子群，它借助于元素1使特征α与它对应. 这就证明了，给定特征α，如果不计同构的话，群G被完全确定. 同时我们也得到，对于任意型$\mathfrak{a}$，可以找到群R的一个子群，使得型$\mathfrak{a}$与它对应.

这样，在一切型和一切互不同构的秩1的无扭群之间建立了一个相互单值对应. 这时R型与群R本身对应，这就是它的名称的由来，零型与无限循环群对应. 如果令$\alpha_n=\infty$，而当$s\neq n$时，$\alpha_s=0$，则这样的特征所构成的型与p_n进分数(即分母是素数p_n的幂的有理数)加法群对应. 我们还要指出，包含特征

$$(1,1,\cdots,1,\cdots)$$

的型与分母不能被任何素数的平方所整除的有理数加法群对应.

如果秩1的无扭群G对应着型$\mathfrak{a}$，那末就说，G是$\mathfrak{a}$型群.

所得到的秩1群的描述是足够清楚和便利的了. 例如，读者不难证明，如果给定两个秩1的无扭群G与H，它们分别对应着型$\mathfrak{a}$与$\mathfrak{b}$，那末群G与群H的一个子群同构，当且仅当$\mathfrak{a}\leqslant\mathfrak{b}$时. 由此推出，如果群$G$与$H$的每一个都与另一个的子群同构，那末这两个群彼此同构. 我们的描述也同时指出了秩1的无扭阿贝尔群的多种多样性，特别，由此推出，所有这些群的集合具有连续统的势.

现在回过来讨论任意无扭阿贝尔群. 设G是这样的一个群而a是它的一个异于零的元素. 由元素a所生成的群G的纯子群A是一个秩1的群，因为正如上面所指出的那样，这个子群的任意元素都与元素a线性相关. 这个子群同时是群G中含有元素a的最大秩1子群. 我们把子群A的型叫做元素a的型. 换句话说，元素a的型是这样的特征的型，这个特征是如此得到的：令$\alpha_n=k$，假如在群G中方程$p_n^k x=a$可解，但方程$p_n^{k+1}x=a$不可解；而令$\alpha_n=\infty$，假如对所有的k来说，形式如$p_n^k x=a$的方程在G中都可

解，此处 $p_n(n=1,2,\cdots)$ 是按递增顺序排列的全体素数. 就是在这个意义下，我们也有时谈论群 G 的元素 a 的特征.

我们现在可以把群 G 的异于零的元素按照它们的型来加以分类，这在某种意义下相当于把准素阿贝尔群的元素分成有限高度和无限高度的分法. 因此，无扭阿贝尔群可以按照它们所包含的元素是什么样的型来分类. 特别，可以分出凡异于零的一切元素都有同一个型 $\mathfrak{a}$ 的那种群来作为特殊的研究对象. 虽然如此，仅仅这样一个限制对于深远理论的发展也是不够的. 不错，容易看出，所有异于零的元素都具有 R 型的群是完备群，因而已经完全被研究了；但是对于所有这样的群，其中一切非零元素都有(比方说是)零型，则尚研究得很少.

我们指出无扭阿贝尔群 G 的元素的型的某些性质，这些性质在下一节要用到.

I. 两个彼此线性相关的元素具有同一型.

事实上，这两个元素生成同一个纯子群.

II. 若元素 a 与 b 分别具有型 $\mathfrak{a}$ 与 $\mathfrak{b}$，那末和 $a+b$(如果它异于零的话)的型大于或等于 $\mathfrak{ab}$.

事实上，设元素 a 与 b 的特征分别是 α 与 β，那末元素 $a+b$ 在任何情况下都可以被素数 p_n 的指数不大于 $\min(\alpha_n,\beta_n)$ 的幂所整除. 但是，可用简单的例子指出，假如数 α_n 与 β_n 都是有限的且彼此相等，那末这个元素也可以被数 p_n 的较高次幂所整除.

III. 若 $G=A+B, a\in A, b\in B$，并且元素 a 与 b 的型分别是 $\mathfrak{a}$ 与 $\mathfrak{b}$，那末元素 $a+b$ 的型等于乘积 $\mathfrak{ab}$.

事实上，在这一情形下元素 $a+b$ 的特征 γ 是这样的，对所有 n 来说，都有 $\gamma_n=\mathrm{mim}(\alpha_n,\beta_n)$.

设 G 是一个无扭阿贝尔群而 $\mathfrak{a}$ 是任意一个型. 用 $G(\mathfrak{a})$ 来表示由零和群 G 中一切型大于或等于 $\mathfrak{a}$ 的元素所成的集合；如果这

样的元素不存在，那末$G(\mathfrak{a})=0$. 由 II 得出，$G(\mathfrak{a})$是群G的子群，而 I 表明，这个子群是G的纯子群. 用$G'(\mathfrak{a})$表示由群G中一切这样的元素，它们的型严格大于$\mathfrak{a}$，所生成的子群. 这个子群包含在子群$G(\mathfrak{a})$中，也有时与它重合；但是在一般情形下，它不一定是$G(\mathfrak{c})$中的纯子群. 因此，商群

$$G^*(\mathfrak{a})=\frac{G(\mathfrak{a})}{G'(\mathfrak{a})}$$

可能包含有限阶的元素.

我们所引入的子群$G(\mathfrak{a})$，$G'(\mathfrak{a})$以及商群$G^*(\mathfrak{a})$在下一节都要用到.

§31. 完全分解群

我们在前一节里研究了秩 1 的无扭群之后，自然就要转到可分解成秩1群的直和的无扭阿贝尔群的研究；这样的群叫做*完全分解群*. 这一类的群已经是足够广泛的了——除了所有秩 1 群以外，一切自由阿贝尔群以及一切完备无扭群都属于这一类. 另一方面，以后我们就会看到，完全分解群也还远远未能穷尽所有无扭阿贝尔群.

关于一个无扭群是不是完全分解群，存在着各种判别法(参看 Baer[15]，Ляпин[6]). 但是所有这些判别法都表述得非常繁赘同时也都不能用来更进一步地发展完全分解群的理论；因此我们不来叙述它们. 对完全分解群来提出关于子群或商群的问题也是不合适的：任何一个无扭阿贝尔群都包含在某一完备无扭群内并且是某一自由群的商群. 因此，我们只讨论完全分解群的直分解的一些性质，并且从以下的定理开始(Baer[15]).

若无扭阿贝尔群G是完全分解群，那末这个群的任意两个分成秩 1 群的直和分解彼此同构.

事实上，设给定了群 G 的任意一个分成秩 1 群的直和分解：

$$G=\sum_{\alpha}A_{\alpha}. \tag{1}$$

如果群 G 含有型 $\mathfrak{a}$ 的元素，那末子群 $G(\mathfrak{a})$（参看前一节的末尾）与分解(1)中这样的被加群的直和重合，这些群的型大于或等于 $\mathfrak{a}$. 事实上，由于直被加群都是纯子群，子群 A_α 中任意一个非零元素的型都等于这个子群本身的型，然后再利用前一节的性质I—III. 类似地，子群 $G'(\mathfrak{a})$ 与分解(1)中这样的被加群的直和重合，它们的型严格大于型 $\mathfrak{a}$. 由此推出，分解(1)中型等于 $\mathfrak{a}$ 的被加群的直和与商群 $G^*(\mathfrak{a})$ 同构，这就是说，与分解(1)的选择无关：在群 G 分成秩 1 群的直和的任意一个分解中所包含的型 $\mathfrak{a}$ 的被加群和群 $G^*(\mathfrak{a})$ 的秩一样多，假如这个秩是有限的话，或者和群 $G^*(\mathfrak{a})$ 的势相同，假如它的秩是无限的话. 定理证毕.

发生这样的问题，完全分解群的任意一个直分解是否都可以继续分解为秩 1 群的直和？换句话说，完全分解群的任意一个直被加群是不是完全分解的？关于这个问题的最终答案还没有得到.[1] 在贝尔(Baer)的论文[15]中包含了关于这问题的一系列特殊结果，其中某些结果即将加以阐述.

我们首先考察可分解成同构的秩 1 群的直和的这种群，并且证明以下定理：

设无扭阿贝尔群 G 有一个直分解

$$G=\sum_{\alpha}A_{\alpha}, \tag{2}$$

其中所有被加群 A_α 都有秩 1 及同一型 $\mathfrak{a}$，又设 B 是 G 的一个纯子群，那末 B 可以分解为秩 1 且有同一型 $\mathfrak{a}$ 的群的直和.

1) 到准备第三版时，这个问题的答案已得到，[参看补充 31.4.]

假设指数 α 遍历所有小于某一 σ 的序数，并且引入以下记法：

$$G^{(\beta)}=\sum_{\alpha<\beta}A_\alpha,$$

$$B^{(\beta)}=B\cap G^{(\beta)}.$$

对于任意 β，包含关系

$$B^{(\beta)}\subseteq B^{(\beta+1)}$$

成立，并且或者等号成立，或者商群 $\frac{B^{(\beta+1)}}{B^{(\beta)}}$ 有秩 1 及型 $\mathfrak{a}$. 事实上，这个商群与商群 $\frac{G^{(\beta+1)}}{G^{(\beta)}}$ 的子群同构，而后者与群 A_β 同构，这就是说，它有秩 1 而型小于或等于 $\mathfrak{a}$. 另一方面，如果子群 $B^{(\beta+1)}$ 包含一个不在 $B^{(\beta)}$ 中的元素 x，那末，由于 B 是纯子群，这个元素在 B 中的型，因而在 $B^{(\beta+1)}$ 中的型等于 $\mathfrak{a}$. 因此，这个元素在商群 $\frac{B^{(\beta+1)}}{B^{(\beta)}}$ 中的型不能小于 $\mathfrak{a}$，我们的论断被证明.

如果证明了，对于 $B^{(\beta)}\neq B^{(\beta+1)}$，直分解

$$B^{(\beta+1)}=B^{(\beta)}+C_\beta \tag{3}$$

成立，此处 C_β 是秩 1 及型 $\mathfrak{a}$ 的群，那末定理就被证明了，因为子群 B 与一切异于零的子群 $C_\beta, \beta<\sigma$, 的直和重合. 因此，我们转来证明分解(3)的存在.

在子群 $B^{(\beta+1)}$ 中选取一个不在子群 $B^{(\beta)}$ 中的元素 x，并且用 $\bar{x}$ 来表示陪集 $x+B^{(\beta)}$. 如果元素 x 在群 $B^{(\beta+1)}$ 中能被某一数 n 整除，那末元素 $\bar{x}$ 在群 $\frac{B^{(\beta+1)}}{B^{(\beta)}}$ 中也能被同一个数所整除. 反过来可能不成立，但是由元素 x 与 $\bar{x}$ 有相同的型这一事实推出，只存在有限多个素数

$$p_{i_1}, p_{i_2}, \cdots, p_{i_s}, \tag{4}$$

使得对于素数 $p_{i_k}(k=1, 2, \cdots, s)$ 来说，元素 x 的特征的值 α_{i_k} 异于元素 $\bar{x}$ 的特征的值 $\bar{\alpha}_{i_k}$，同时这两个数都是有限的且

$$\bar{\alpha}_{ik}<\bar{a}_{ik}.$$

令
$$\bar{h}=p_{i_1}^{\bar{\alpha}_{i_1}}p_{i_2}^{\bar{\alpha}_{i_2}}\cdots p_{i_s}^{\bar{\alpha}_{i_s}},$$
$$h=p_{i_1}^{\bar{\alpha}_{i_1}-\alpha_{i_1}}p_{i_2}^{\bar{\alpha}_{i_2}-\alpha_{i_2}}\cdots p_{i_s}^{\bar{\alpha}_{i_s}-\alpha_{i_s}}.$$

在群$\frac{B^{(\beta+1)}}{B^{(\beta)}}$中存在这样的元素 $\bar{y}=y+B^{(\beta)}$，使得

$$\bar{h}\bar{y}=\bar{x}, \tag{5}$$

这就是说，元素 x 与 $\bar{h}y$ 属于同一陪集 $\bar{x}$. 令数 h' 对于元素 $\bar{h}y$ 扮演着数 h 对于元素 x 的角色. 但是，由元素 $\bar{h}y$ 能被数 $\bar{h}$ 整除推出，数 h' 不能被(4)中的任何一个素数整除，所以

$$(h, h')=1.$$

因此，存在这样的整数 l 及 l' 使得

$$lh+l'h'=1. \tag{6}$$

根据(5)和(6)，元素

$$z=lhx+l'h'(\bar{h}y) \tag{7}$$

属于陪集 $\bar{x}$. 如果p_j 是任意一个素数而β_j 是元素 z 的特征对于这个素数的值，那末显然 $\beta_j\leqslant\bar{\alpha}_j$. 但是元素 z 在任何情况下都可以被数 p_j 的这样的幂所整除，这个幂可以整除等式(7)右边的两个被加项，因此，应用数 h 与 h' 的定义，我们得到 $\beta_j\geqslant\bar{\alpha}_j$.

这样，在陪集 $\bar{x}$ 里，我们找到了这样的元素 z，它在群 $B^{(\beta+1)}$中的特征和元素 $\bar{x}$ 在群$\frac{B^{(\beta+1)}}{B^{(\beta)}}$中的特征一致. 因此，如果我们用 C_β 表示群 $B^{(\beta+1)}$中由元素 z 所生成的纯子群，那末在群 $B^{(\beta+1)}$对子群 $B^{(\beta)}$ 的每一陪集里都包含 C_β 中的一个元素. 这就证明了直分解(3)的存在. 定理证毕.

取群 G 的一个直被加群作为 B 而应用这个定理，我们得到这样的结果：

若群 G 被分解成秩 1 并且有同一型 $\mathfrak{a}$ 的直和，那末这个群的

任意一个直被加群也被分解成秩 1 及型 $\mathfrak{a}$ 的群的直和.

现在我们证明以下更一般的定理[1].

设 G 是一个完全分解群并且在它被分成秩 1 群的直和分解

$$G=\sum_{\alpha}A_{\alpha} \tag{8}$$

中，被加群的型的集合是有限的. 那末群 G 的任何一个直被加群本身都是完全分解群.

为了证明这个定理,我们用

$$\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n \tag{9}$$

表示出现在分解(8) 中被加群的一切不同的型，而用 $D_i(i=1,2,\cdots,n)$表示这个分解中型是 $\mathfrak{a}_i$ 的被加群的直和. 那末

$$G=D_1+D_2+\cdots D_n. \tag{10}$$

如果我们能证明,分解(10)与群 G 的任意直分解,

$$G=\sum_{\beta}B_{\beta}, \tag{11}$$

具有同构的延拓,那末定理就证明了. 事实上，在这一情形下,任意 B_β 都将被分解成与群 $D_i(i=1,2,\cdots,n)$的直被加群同构的子群的直和,因而正如上面所证明了的,它是完全分解群.

我们对数 n 用归纳法来证明直分解(10)与(11)的同构延拓的存在,因为当 $n=1$ 时是用不着证明的. 设型 $\mathfrak{a}_1$ 是(9)中最大型(在型的半序意义下)之一. 那末子群 D_1 在第二个分解的直被加群 B_β 中的分支与交

$$C_\beta=D_1\cap B_\beta$$

重合;它不可能大于这个交,因为任何子群都同态地被映到它自己的分支上,但是由于型 $\mathfrak{a}_1$ 的选取,子群 D_1 中任何元素无论在这个

1) 证明是 Л. Я. Куликов 告诉作者的.

子群的哪一个同态之下都不可能映成群 G 的不属于 D_1 的元素. 由此推出，存在直分解

$$D_1=\sum_\beta C_\beta,$$

这就是说，我们得到分解(10)的如下的接续:

$$G=\sum_\beta C_\beta+D_2+\cdots+D_n. \tag{12}$$

子群 B_β 包含群 G 的直被加群 C_β，因此对于任意 β 都存在直分解

$$B_\beta=C_\beta+C'_\beta,$$

这就是说，我们得出分解(11)的如下的接续:

$$G=\sum_\beta C_\beta+\sum_\beta C'_\beta. \tag{13}$$

分解(12)和(13)表明，子群

$$D_2+\cdots+D_n,\quad \sum_\beta C'_\beta \tag{14}$$

彼此同构，因此根据归纳假定，对分解(14)来说，存在同构接续. 把它们分别代入(12)和(13)，我们就得到分解(10)和(11)的同构延拓，这也就是所要证明的.

由这个定理还推出，*有限秩的完全分解群的任何一个直被加群本身也是完全分解群.*

关于完全分解群的直被加群的问题，实际上得到了比上面所述的较进一步的一些结果. 例如，Baer[15]证明了，当上面定理的陈述中分解(8)的被加群的型的集合不一定是有限的，而只是满足极大条件(在型的偏序意义下)的时候，直被加群有完全分解性. 另一方面，Куликов 证明了，任意可数完全分解群的直被加群是完全分解的. [参看补充 31.4.]

§32. 无扭阿贝尔群的其他一些类

到目前为止，我们还没有遇到过不是完全分解群的无扭阿贝尔群．以下定理说明它们的存在．

无限多个无限循环群的完全直和(参看§17)不是完全分解群．

事实上，设群 G 被表成无限循环群的完全直和的形式，这些无限循环群的集合具有无限的势 $\mathfrak{m}$．在这个集合里选出一个可数的子集合并且把出现在这个子集合内的子群的完全直和记作 G'．如果群 G 是完全分解的，那末，由于它的所有元素都有零型，它将是一个自由群，因而与群 G 的某一子群同构的群 G' 也是一个自由群．因此我们可以认为，群 G 本身是可数个无限循环群的完全直和．设

$$a_1, a_2, \cdots, a_n, \cdots$$

是这些循环群的生成元，那末群 G 的任何一个元素 g 都可以写成这些生成元取整系数的无限多项的和的形式：

$$g = k_1a_1 + k_2a_2 + \cdots + k_na_n + \cdots \tag{1}$$

用 H 表示具以下性质的形式如(1)的元素的全体：对于任意自然数 s，几乎所有系数 $k_1, k_2, \cdots, k_n, \cdots$(这就是说，除去可能的有限多个外，所有的系数)都能被 2^s 整除．集合 H 是群 G 的子群，它正如 G 本身一样，具有连续统的势．如果群 G 是自由群，那末 H 也是自由群，即有连续统那样多的无限循环群的直和，而这时商群 $\frac{H}{2H}$，此处 $2H$ 是群 H 中一切在这个群中可以被数 2 整除的元素的全体，也应该具有连续统的势．

然而实际上，商群 $\frac{H}{2H}$ 是可数的．事实上，群 H 包含一个可数子群 H'，它是由形式如(1)但是只有有限多个非零系数 k_n 的元素

所构成的. 现在假设 h 是 H 的任意元素，那末由它减去 H' 中这样的元素 h'，使得差 $h-h'$ 写成形式(1)时所有系数都能被 2 整除. 这样，

$$h-h'=2h_0,$$

并且，容易看出，元素 h_0 属于子群 H，即

$$h-h'\subset 2H.$$

这就证明了，群 H 对子群 $2H$ 的任意一个陪集都包含子群 H' 的元素，这就证明了商群 $\frac{H}{2H}$ 的可数性.

用同样的方法可以证明(Baer[15])，一般来说，任意无限多个秩1的、具有同一型、而这个型不等于 R 的群的完全直和，都不可能是完全分解群. 更进一步，在 Мишина 的论文[1]里证明了，若群 G 是若干秩 1 群 A_α(α 遍历某一足标集合 M)的完全直和，那末 G 是完全分解群当且仅当在群 A_α 中只有有限多个非 R 型的群. [参看补充 31. 5.]

上面所构成的群，虽然不是完全分解群，却是可分解成直和的——从循环群的完全直和中，总可以裂分出循环直被加群. 然而也存在这样的无扭阿贝尔群，它们的秩大于 1 同时并不能分解成直和. 这是由于以下的定理(Baer[15]).

p 进整数(参看 §21) 加法群 J 的任何一个纯子群 C 是不可分解的；特别地，群 J 本身是不可分解的.

事实上，我们考虑由群 J 的一切元素的 p 倍所作成的子群 pJ. 这个子群刚好包含一切这样的 p 进整数，它们在 §21 的形式(9)的写法中第一位是零，即 $k_1=0$. 由此推出，子群 pJ 在群 J 中的指数等于 p.

因此，子群 pC 在群 C 中的指数也等于 p，这就是说，商群 $\frac{C}{pC}$ 是 p 阶循环群. 事实上，

$$pC = C \cap pJ,$$

因为子群 C 是 J 中的纯子群，而

$$J = C + pJ,$$

这是因为 pJ 在 J 中的指数是素数 p，再应用同构定理，即

$$\frac{C}{pC} \simeq \frac{J}{pJ}.$$

如果子群 C 可分解，

$$C = C_1 + C_2,$$

那末子群 C_1 与 C_2 作为纯子群的直被加群，它们本身也是 J 中的纯子群，因此商群 $\frac{C_1}{pC_1}$ 与 $\frac{C_2}{pC_2}$ 都将是 p 阶循环群. 但是

$$pC = pC_1 + pC_2,$$

因而商群 $\frac{C}{pC}$ 是两个 p 阶循环群的直和，这与上面所证明的事实矛盾.

因为群 J 有连续统的势，所以在其中可以找到任意有限秩的纯子群，也可以找到任意不超过连续统的势的无限秩的纯子群. 关于不能分解成直和的具任意无限势的无扭阿贝尔群是否存在的问题目前尚未解决. [1]

在 Baer 的论文[15]中还研究了无扭阿贝尔群的某些类，它们非常近似于完全分解群. 例如，无扭阿贝尔群 G 叫做*可分离的*，假如群 G 的任意有限多个元素都包含在这个群的一个完全分解的直被加群内；自然，可以认为所说直被加群具有限的秩. 显然，每一个完全分解群都是可分离的.

任何一个可数的可分离群 G 都是完全分解群.

事实上，设 $g_1, g_2, \cdots, g_n, \cdots$ 是群 G 的所有元素. 令 $A_0 = 0$. 假设在 G 中已经找到包含元素 $g_1, g_2, \cdots, g_n$ 的有限秩的完全分解直

1) 到准备第三版时，这个问题的答案已得到。[参看补充 31.2.]

被加子群 A_n. 作为子群 A_{n+1}，我们取群 G 的这样一个完全分解直被加群，它具有限秩并且它既包含元素 g_{n+1} 且又包含子群 A_n 的某一个极大线性无关元素系. 那末，由于 A_{n+1} 是 G 的纯子群，A_n 包含在 A_{n+1} 内，因而也是 A_{n+1} 的一个直被加群:

$$A_{n+1}=A_n+B_{n+1}.$$

子群 B_{n+1} 作为有限秩的完全分解群的直被加群，本身也是完全分解群(参看前一节). 群 G 与递增子群序列 A_n, $n=0,1,2,\cdots$, 的并集重合，因而是完全分解群 $B_n(n=1,2,\cdots)$ 的直和，这就是说，G 本身是完全分解群.

在不可数的情形下，存在可分离的但不是完全分解的群: 无限多个无限循环群的完全直和是可分离群，虽然，如以上所证，它不是完全分解群.

事实上，设群 G 是具生成元 a_α(α 遍历某一足标集合)的无限循环群的完全直和. 我们首先证明，群 G 的任意元素 g 都包含在这个群的一个完全分解的直被加群中: 显然，可以认为 $g\neq 0$. 元素 g 可以写成

$$g=\sum_\alpha k_\alpha a_\alpha, \tag{2}$$

此处 k_α 是整数. 用 $k(g)$ 表示所有异于零的系数 k_α 的绝对值中最小的，

$$k(g)=\min(|k_\alpha|, k_\alpha\neq 0).$$

如果 $k(g)=1$，那末有这样的指数 β，值 $k_\beta=\pm 1$. 于是

$$G=\{g\}+G',$$

此处子群 G' 是由群 G 中一切这样的元素组成的，这些元素在形式如(2)的写法中，a_β 的系数等于零; 因此，G' 本身也是无限循环群的完全直和.

现在设 $k(g)$ 是任意的. 把(2)中每一个系数 k_α 用 $k(g)$ 去除:

$$k_\alpha = k(g)q_\alpha + r_\alpha, \quad 0 \leqslant r_\alpha < k(g).$$

于是

$$g = k(g)g_1 + g_2,$$

此处

$$g_1 = \sum_\alpha q_\alpha a_\alpha,\ g_2 = \sum_\alpha r_\alpha a_\alpha.$$

因为有这样的 β，使 $k(g) = \pm k_\beta$，所以 $q_\beta = \pm 1$ 因而 $k(g_1) = 1$. 因此，直分解

$$G = \{g_1\} + G'$$

成立，并且 G' 包含 G 中所有这样的元素，在它们的写法中 a_β 的系数等于零. 元素 g_2 也是这样的元素，即 $g_2 \in G'$. 但是 $k(g_2)$ 严格地小于 $k(g)$，——要知道所有系数 r_α 都严格地小于 $k(g)$. 因此可以认为，我们证明了存在这样的直分解

$$G' = A + B,$$

使得 A 包含 g_2 并且是完全分解群，它甚至还是一个有限秩自由群，而子群 B 由群 G 中一切这样的元素所组成，在它们的写法(2)中某些取定的有限多个 a_α 的系数等于零. 元素 g 现在包含在群 G 的完全分解的直被加群 $\{g_1\} + A$ 内.

最后，如果在群 G 中给出一组有限个元素 $g_1, g_2, \cdots, g_n$，那末可以认为，我们证明了存在直分解

$$G = U + V,$$

此处 U 是包含元素 $g_1, g_2, \cdots, g_{n-1}$ 的完全分解直被加群，而 V 是无限循环群的完全直和. 于是

$$g_n = u + v,\ u \in U,\ v \in V,$$

但因为，根据所证明的，存在这样的直分解

$$V = A + B,$$

使得 A 是包含 v 的一个完全分解群，所以群 G 的直被加群 $U + A$

也是完全分解的并且包含所有给定的元素；同时直被加群 B 是无限循环群的直和．群 G 的可分离性被证明．［参看补充 31.5.］

在 Baer 的论文[15]中还研究了另外几类无扭阿贝尔群，特别是这样的群的直和，它们的所有异于零的元素都具有同一的型．正如 Конторович 的论文[7]所证明了的，这一类群的理论可以推广到这样的无扭非交换群上，在其中，如同在所有的无扭阿贝尔群中一样，方程

$$x^n = a, n > 0,$$

不能有多于一个的解．

有限秩的群的研究构成无扭阿贝尔群理论中一个特殊的方向．在本章下面几节里，我们要阐述研究这种群的一些方法和必要的补充知识．特别提出关于有限秩无扭阿贝尔群被分成不可分解群的直和的同构这样的有趣问题．在 Jónsson[1] 的文章中举例说明，这样的同构不是永远存在的．［参看补充．31.3.］

§32a p 进数域

在以下几节里，我们将用到有理数域的一个扩域，它在代数的许多分支里都扮演着重要的角色．在这里，我们要定义这个扩域，并且指出它的一些对今后讨论所需要的一些主要性质．

取定一个素数 p．在整个这一节里，这个 p 都是固定的，并且在有理数域 $\mathfrak{R}$ 内定义一个 p 进范数．如果 a 是一个有理数，$a \neq 0$，那末 a 可以写成

$$a = a' p^n,$$

这里 a' 是一个既约分数，它的分子和分母都与 p 互素，n 是一个整数，可以大于、等于或小于零．数 p^{-n} 叫做数 a 的 p 进范数，记作

$$\|a\| = p^{-n}.$$

此外，我们再约定$\|0\|=0$. 那末对于任意一个有理数a,都有一个非负数与它对应. 当$a\neq 0$时,这个数不等于零,并且

$$\|ab\|=\|a\|\cdot\|b\|, \tag{1}$$

$$\|a+b\|\leqslant\max(\|a\|,\|b\|). \tag{2}$$

在后一个关系里,<符号仅当$\|a\|=\|b\|$时才有可能出现. 再者,由于$\|-a\|=\|a\|$,所以

$$\|a-b\|\leqslant\max(\|a\|,\|b\|).$$

我们现在利用p进范数来定义有理数域的一个扩域，就如同按照Cantor的方法利用有理数的绝对值构造实数域的情形一样，有理数序列$a_1,a_2,\cdots,a_n,\cdots$, 不一定互不相同，说是(在$p$进范数意义下)收敛的，如果对于任意给定的正有理数$\varepsilon$，总存在一个自然数$m$,使得

$$\|a_i-a_j\|<\varepsilon, \text{如果 } i>m, j>m.$$

有理数b叫做有理数序列$b_1,b_2,\cdots,b_n,\cdots$的($p$进)极限，如果对于任意$\varepsilon>0$,存在一个$m$,使得

$$\|b-b_i\|<\varepsilon, \text{如果 } i>m.$$

容易看出，任何一个有极限的序列一定是收敛的. 然而反过来不一定对. 例如,序列

$$1, 1+p, 1+p+p^2, 1+p+p^2+p^4, \cdots$$
$$\cdots, 1+p+p^2+\cdots+p^{2(n-1)}+p^{2n}, \cdots$$

是收敛的,但没有极限.

两个收敛序列(a_n)与(b_n)的和与积指的是序列(a_n+b_n)与(a_nb_n). 容易验证,这两个序列仍是收敛的[1]，并且我们所定义的收敛序列的加法与乘法满足交换环定义里的全部要求.此外,如果

1) 在证明序列(a_nb_n)的收敛性时,注意到序列(a_n)与(b_n)的元素的范数都是有上界的。

序列(a_n)与(b_n)分别有极限a与b，那末序列(a_n+b_n)有极限$a+b$，序列(a_nb_n)有极限ab.

具有极限0的序列在所有收敛序列的环$\mathfrak{K}$里构成一个理想，我们把这个理想记作$\mathfrak{N}$. 商环

$$\mathfrak{P}=\mathfrak{K}/\mathfrak{N}$$

是域. 事实上，如果给定一个不含在$\mathfrak{N}$内的收敛序列(a_n)，那末存在这样的有理数$\eta>0$和自然数k，使得对于一切$i>k$都有$\|a_i\|>\eta$. 如果把序列(a_n)的前k个元素都换成范数大于η的数，我们得到一个序列$(\bar{a}_n)$，它与(a_n)属于关于理想$\mathfrak{N}$的同一剩余类，而在序列$(\bar{a}_n)$里，对于所有的i，都有$\|\bar{a}_i\|>\eta$，特别，$\bar{a}_i\neq 0$. 现在考察序列$(\bar{a}_n^{-1})$. 这个序列也是收敛的，因为由

$$\|\bar{a}_i-\bar{a}_j\|<\varepsilon, \text{对于 } i>m, j>m,$$

可以得到

$$\|\bar{a}_j^{-1}-\bar{a}_i^{-1}\|=\|(\bar{a}_i-\bar{a}_j)\bar{a}_i^{-1}\bar{a}_j^{-1}\|<\varepsilon\eta^{-2}.$$

与此同时，序列$(\bar{a}_n)$与序列$(\bar{a}_n^{-1})$的乘积是序列$(1,1,\cdots)$，它是环$\mathfrak{K}$的单位元. 这就证明了在$\mathfrak{P}$中每一个非零元素都有逆元.

域$\mathfrak{P}$叫做p进数域，它的元素叫做p进数. 这个域包含有理数域$\mathfrak{R}$. 为了证明这一点，我们把每一个有理数a与含有收敛序列$(a,a,\cdots)$的关于理想$\mathfrak{N}$的剩余类等同起来，这个类由一切以数a为极限的序列组成. 不难证明，域$\mathfrak{R}$到域$\mathfrak{P}$内的这个映射是同态单射.

在域$\mathfrak{P}$里定义范数，作为域$\mathfrak{R}$里p进范数的开拓，也就是说，这个范数在域$\mathfrak{R}$里与原有的p进范数一致. 设α是由收敛序列$a_1,a_2,\cdots,a_n,\cdots$所定义的一个不等于零的$p$进数. 我们来证明，范数$\|a_1\|,\|a_2\|,\cdots,\|a_n\|\cdots$，从某一个$n$开始都相等. 事实上，如果

$$\|a_i-a_j\|<\varepsilon \quad \text{对于 } i>m, j>m,$$

那末当$\|a_i\| \neq \|a_j\|$时，由

$$\|a_i - a_j\| = \max(\|a_i\|, \|a_j\|)$$

推出，$\max(\|a_i\|, \|a_j\|) < \varepsilon$. 因此，若是对于任意 n，都存在这样的 $i > n$, $j > n$，使得$\|a_i\| \neq \|a_j\|$，就将与$\alpha \neq 0$ 的假设相违，所以一定存在这样的 n，使得

$$\|a_n\| = \|a_{n+1}\| = \cdots = p^k.$$

现在令$\|\alpha\| = p^k$. 这个定义不依赖于序列 $a_1, a_2, \cdots, a_n, \cdots$ 的选取，因为如果序列 $b_1, b_2, \cdots, b_n, \cdots$ 有极限零，即$(b_n) \in \mathfrak{N}$，那末对于大于某一个 m 的所有的 i，都有$\|b_i\| < p^k$，从而

$$\|a_i + b_i\| = p^k, \text{若} \quad i > m.$$

序列$(a_n + b_n)$仍然定义数α. 这样，$(a_n + b_n)$与(a_n)给出α的同一个范数. 再约定$\|o\| = 0$. 于是在域 $\mathfrak{P}$ 里就引进了范数，它对于有理数来说与原有的范数一致，并且条件(1)和(2)仍然被满足.

现在籍助于所引进的范数，就可以在域p里定义序列的收敛概念和极限概念，也就是说，把以前所给的关于序列的收敛和极限的定义搬到这里来. 容易验证，每一个 p 进数 α 都是用来定义它的有理数序列(a_n)的极限. 不仅如此，我们还有以下的定理.

I. *在域 $\mathfrak{P}$ 里，每一个收敛序列都有极限.*

事实上，设给定 p 进数的收敛序列 $\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$. 对于每一个 n，可以找到这样一个有理数 a_n，使得

$$\|\alpha_n - a_n\| < \frac{1}{n}.$$

因此，

$$\|a_i - a_j\| = \|(a_i - \alpha_i) + (\alpha_i - \alpha_j) + (\alpha_j - a_j)\|$$
$$\leqslant \max\left(\frac{1}{i}, \|\alpha_i - \alpha_j\|, \frac{1}{j}\right).$$

这就是说，对于足够大的 i 和 j，这个范数可以任意小. 所以序列(a_n)收敛，从而它定义了一个 p 进数 β. 由于

$$\|\beta-\alpha_n\|=\|(\beta-a_n)+(a_n-\alpha_n)\|$$
$$\leqslant\max\left(\|\beta-a_n\|,\frac{1}{n}\right),$$

所以 β 是序列 (α_n) 的极限.

为了以后的讨论，需要在域 $\mathfrak{P}$ 里定义某些初等拓扑的概念. $\mathfrak{P}$ 的一个子集(特别,一个子环) $\mathfrak{M}$ 说是*闭的*，如果属于 $\mathfrak{M}$ 的元素的每一个收敛序列的极限都在 $\mathfrak{M}$ 内. 如果集 $\mathfrak{M}$ 不是闭的,那末容易看出,把属于 $\mathfrak{M}$ 的元素所有收敛序列的极限都添加到 $\mathfrak{M}$ 上所得的子集 $\overline{\mathfrak{M}}$ 就是闭的; $\overline{\mathfrak{M}}$ 叫做集 $\mathfrak{M}$ 的*闭包*. 最后, $\mathfrak{P}$ 的子集 $\mathfrak{M}$ 说是*紧的*，如果属于 $\mathfrak{M}$ 的元素的每一个序列都含有一个收敛的子序列,它的极限在 $\mathfrak{M}$ 内.

因为每一个 p 进数都是有理数序列的极限,所以有

II. *有理数域 $\mathfrak{R}$ 在 $\mathfrak{P}$ 内的闭包等于 $\mathfrak{P}$.*

更进一步,还可以证明

III. *域 $\mathfrak{P}$ 是 p 进分数环 $\mathfrak{R}_p$ 的闭包.*

因为每一个 p 进数都是有理数序列的极限,所以只需证明,每一个有理数都是由环 $\mathfrak{R}_p$ 的数所组成的序列的 p 进极限. 设给定一个有理数 $\frac{m}{n}$, 又令 s 是一个正整数. 如果 $n=p^k n_0$, $(n_0,p)=1$, $k\geqslant 0$, 那末选取整数 v, 使它满足同余式

$$n_0 v\equiv m \pmod{p^{s+k}}.$$

于是

$$\left\|\frac{m}{n}-\frac{v}{p^k}\right\|=\left\|\frac{m-n_0 v}{n}\right\|\leqslant p^{-s},$$

而 $\frac{v}{p^k}\in\mathfrak{R}_p$. 论断 III 被证明.

p 进数 α 说是*整的*,如果 $\|\alpha\|\leqslant 1$. 由 p 进范数的性质(1)和(2)可以推出, p 进整数的和、差、积仍是整的，即 *p 进整数构成一个*

环．这个环在§21已经以另一种形式出现过，以后将把它记作$\mathfrak{S}$．下面两个论断是明显的：

IV．环$\mathfrak{S}$与有理数域$\mathfrak{R}$的交是由分母与p互素的一切有理数所组成的环$\mathfrak{R}^{(p)}$．

V．环$\mathfrak{S}$与p进分数环$\mathfrak{R}_p$的交是有理整数环$\mathfrak{C}$．

由III和V不难得出以下定理：

VI．环$\mathfrak{S}$是环$\mathfrak{C}$的闭包．

事实上，如果给定一个不等于零的p进整数α，那末根据III，它是一个p进分数收敛序列$a_1, a_2, \cdots, a_n, \cdots$的极限．因为$\alpha \neq 0$，所以从某一个$n$开始，范数$\|a_n\|$都等于$\alpha$的范数，即小于或等于1，于是由V，数$a_n$是有理整数．反之，任何有理整数收敛序列的极限的范数都不大于1，即是一个p进整数．

由此得

VII．环$\mathfrak{S}$在域$\mathfrak{P}$里是闭的．

现在设α是一个p进整数而$a_1, a_2, \cdots, a_n, \cdots$是一个以$\alpha$为极限的有理整数序列．把每一个数$a_n$按升幂写成数$p$的幂的和，系数是$0, 1, \cdots, p-1$中之一，并且令$a_n^{(k)}$表示$a_n$的这个写法里从开始截止到$p^k$项，这里$k$是一个非负整数．由序列$(a_n)$的收敛性推出，所有的$a_n^{(k)}$，除去可能的有限多个数外，都彼此相等，即等于一个数，我们把它记作$a^{(k)}$．容易验证，对于所有的k，$a^{(k)}$是$a^{(k+1)}$的前段（按p的升幂书写），而$a^{(k)}$不依赖于序列(a_n)的选取，即是由数α本身所确定的．最后，序列$(a^{(k)})$也以α为极限．现在对于数α，可以有唯一确定的关于数p的升幂的级数与它对应，这个级数的前$k+1$项截断是数$a^{(k)}$，$k=0, 1, 2, \cdots$．这个级数叫做数α的典范写法．反之，每一个关于数p的升幂的级数，它的系数是按模p约化的非负整数，都对应着一个p进整数，这个p进整数是这个级数的截断所成的（收敛）序列的极限．由此得

VIII. 环 $\mathfrak{J}$ 具有连续统的势.

现在证明以下定理:

IX. 环 $\mathfrak{J}$ 是紧的.

设给定一个 p 进整数可数序列

$$\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \qquad (F)$$

因为在这些数的典范写法里,作为 p^0 的系数只能是数 $0, 1, \cdots, p-1$ 中之一,所以在 (F) 里,可以选出无限序列

$$\alpha_1^{(1)}, \alpha_2^{(1)}, \cdots, \alpha_n^{(1)}, \cdots \qquad (F_1)$$

其中每一个数的典范写法里, p^0 的系数都相等. 假设已经确定了序列

$$\alpha_1^{(k)}, \alpha_2^{(k)}, \cdots, \alpha_n^{(k)}, \cdots \qquad (F_k)$$

其中每一个数的典范写法里, $p^0, p^1, p^2, \cdots, p^{k-1}$ 的对应系数都彼此相等. 从这个序列里再选出一个无限序列 (F_{k+1}), 在它的元素的典范写法里, p^k 的系数都相等. 这样对于所有的 k, 定义了序列 (F_k) 的递降链. 现在容易验证,序列

$$\alpha_1^{(1)}, \alpha_2^{(2)}, \cdots, \alpha_k^{(k)}, \cdots$$

是收敛的. 注意到 VII,确信这个定理成立.

环 $\mathfrak{J}$ 显然没有零因子且有单位元. 我们考察这个环的理想. 根据 p 进范数的性质(1)和(2)可知, 由所有范数不大于 p^{-n}, $n \geq 0$, 的 p 进整数所成的集 $p^n\mathfrak{J}$ 在 $\mathfrak{J}$ 内构成一个理想. 理想降链 $\mathfrak{J}$, $p\mathfrak{J}, p^2\mathfrak{J}, \cdots$ 实际上穷尽了环 $\mathfrak{J}$ 的一切非零理想: 如果两个 p 进整数具有同一范数, 那么它们之中的每一个数都含于另一个数所生成的理想内,内为它们的商有范数 1,所以属于 $\mathfrak{J}$. 由此得到

X. 在环 $\mathfrak{J}$ 里,所有的理想都是主理想.

下面关于理想链的性质对我们来说是重要的.

XI. 如果 p 进数收敛序列 $\alpha_1, \alpha_2, \cdots, \alpha_k, \cdots$ 有极限零, 那末每一个理想 $p^n\mathfrak{J}$ 都含有这个序列中除掉可能有限个外的一切数.

XII. 每一个 p 进数都可以通过乘上 p 的一个正整数幂而成为一个 p 进整数.

事实上,如果数 α 的范数是 p^n, $n>0$,那末根据 p 进范数的性质(1),乘积 $p^n\alpha$ 有范数 $\|p^n\alpha\|=1$.

下面我们来考察域 $\mathfrak{P}$ 上有限维向量空间. 设

$$P=\mathfrak{P}u_1+\mathfrak{P}u_2+\cdots+\mathfrak{P}u_n$$

是这样一个向量空间. 在其中如下地定义收敛性: 元素

$$a=\alpha_1u_1+\alpha_2u_2+\cdots+\alpha_nu_n$$

叫做元素

$$a_k=\alpha_{k1}u_1+\alpha_{k2}u_2+\cdots+\alpha_{kn}u_n,\ k=1,2,\cdots,$$

的序列的极限,如果对于每一个 i, $1\leqslant i\leqslant n$,数 α_i 是序列 α_{1i}, α_{2i}, $\cdots$, α_{ki}, $\cdots$的(p 进)极限.

我们这里收敛的定义不依赖于空间 P 的线性无关组 u_1, u_2, $\cdots$, u_n 的选取. 事实上,如果过渡到线性无关组 v_1, v_2, $\cdots$, v_n, 又设

$$u_i=\sum_j\mu_{ij}v_j,$$

那末

$$a=\sum_j\Bigl(\sum_i\alpha_i\mu_{ij}\Bigr)v_j,$$

$$a_k=\sum_j\Bigl(\sum_i\alpha_{ki}\mu_{ij}\Bigr)v_j,\ k=1,2,\cdots$$

因此,在元素 a_1, a_2, $\cdots$里, v_j, $(1\leqslant j\leqslant n)$的系数序列以元素 a 里 v_j 的系数为极限.

现在在空间 P 的加法群里也可以象前面一样地定义闭子集,闭包,紧集等概念. 注意这时一个子群的闭包仍是子群. 事实上,如果 P 的元素 a 是序列 (a_k) 的极限,元素 b 是序列 (b_k) 的极限, 那

末容易验证，序列$(a_k\pm b_k)$有极限 $a\pm b$.

在以下两节里，当引用本节的定理 I—XII 时，我们仅指出定理的号数，而不再指出节数.

§ 326　有限秩无扭群

我们现在将给出有限秩无扭阿贝尔群的完全描述，即描述（确切到同构）有限个同构于有理数加群 R 的群的直和的所有子群. 不同于在 § 30 里对秩为 1 的群所作的描述，任意有限秩的群的情形非常复杂，并且要利用 p 进数. 阿贝尔群与 p 进数的这个联系首先是由 Levi[1]指出的. 对于有限个同构于 p 进分数加群R_p的直和的情形，Курош[6]已经给出了一组完全不变量（即完全描述）. Калужнин[1]利用 p 进数域的拓扑性质，对于这个工作中的某些证明作了简化. Derry[1]研究了任意有限秩无扭阿贝尔群的情形，在那里既用到了 p 进数域的代数性质，也用到了它的拓扑性质. Derry 所作的描述将在本节加以阐明. 用另外一种方法，不要求连续性，而本质上很接近于线性代数的方法对有限秩无扭群的描述是由 Мальцев[1]得到的.

设给出一个有限秩 n 的无扭阿贝尔群 G. 根据 § 23，群 G 包含在一个最小完备群 F 内，这个完备群由群 G 唯一确定，并且它的秩等于 n. 设 $\mathfrak{R}$ 是有理数域. 那末 $F=\mathfrak{R}G$，并且对于 F 的任意元素 x，可以找到 G 中这样一个元素 a 和一个有理数 α（甚至是形如$\frac{1}{m}$的数），使得 $x=\alpha a$. 令 G_p 是群 F 中由元素αa所生成的子群，这里 a 遍历群 G，而 α 是环 $\mathfrak{R}^{(p)}$ 中分母与素数 p 互素的那些有理数，即 $G_p=\mathfrak{R}^{(p)}G$. 子群 G_p 的任意元素可以写成 $\alpha_1a_1+\alpha_2a_2+\cdots+\alpha_ka_k$ 的形式，这里

$$a_1, a_2, \cdots, a_k\in G,\quad \alpha_1, \alpha_2, \cdots, \alpha_k\in\mathfrak{R}^{(p)}.$$

这样的写法可能有多种．注意，对于 $x\in G_p$，$\alpha\in\mathfrak{R}^{(p)}$，元素 αx 也属于 G_p，

$$\mathfrak{R}^{(p)}G_p=G_p.$$

子群 G 是一切子群 G_p 的交，这里 p 取遍所有的素数．

显然，$G\subset G_p$，从而 G 含于一切 G_p 的交内．另一方面，设 b 是这个交的任意一个元素．由于 $b\in G_p$，所以 b 可以写成

$$b=\alpha_1a_1+\alpha_2a_2+\cdots+\alpha_ka_k,$$

这里 $a_1,a_2,\cdots,a_k\in G$，$\alpha_1,\ \alpha_2,\cdots,\alpha_k\in\mathfrak{R}^{(p)}$．如果 r 是数 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 的公分母，那末 $rb\in G$，并且 r 与 p 互素．令 $p_1,p_2,\cdots,p_m$ 是数 r 的一切互不相同的素因子，那末 b 作为子群 $G_{p_1},G_{p_2},\cdots,G_{p_m}$ 的元素，类似地又可以求得这样的整数 $r_1,r_2,\cdots,r_m$，使得 $r_ib\in G$，且 $(r_i,p_i)=1$，$i=1,2,\cdots,m$．于是 $(r,r_1\cdots,r_m)=1$，即存在整数 l，$l_1,\cdots,l_m$，使得

$$lr+l_1r_1+\cdots+l_mr_m=1,$$

由此得

$$b=(lr+l_1r_1+\cdots+l_mr_m)b\in G.$$

现在固定一个素数 p，我们来考虑子群 G_p．如果 $u_1,u_2,\cdots,u_n$ 是群 F 的一个极大线性无关组，那末

$$F=\mathfrak{R}u_1+\mathfrak{R}u_2+\cdots+\mathfrak{R}u_n. \tag{1}$$

我们把群 F 嵌入 p 进数域 $\mathfrak{P}$ 上一个 n 维向量空间

$$P=\mathfrak{P}u_1+\mathfrak{P}u_2+\cdots+\mathfrak{P}u_n.$$

注意空间 P 不依赖于群 F 的直分解(1)的选取，即只由群 G 本身所确定，因为群 F 的另一个直分解仅是导致 P 的一个新的直分解．令 $\overline{G}_p$ 表示子群 G_p 在群 P 内的闭包．我们证明以下定理：

子群 G_p 是群 P 的子群 F 与 $\overline{G}_p$ 的交．

显然，$G_p\subseteq F\cap\overline{G}_p$．另一方面，设元素 x 属于这个交．作为 $\overline{G}_p$ 的元素，它是 G_p 中元素的序列 $x_1,x_2,\cdots,x_k,\cdots$ 的极限，又因为元素

x 和 $x_1, x_2, \cdots, x_k, \cdots$ 都属于 F, 所以下面的等式成立:

$$x=\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n,$$

$$x_k=\alpha_{k1}u_1+\alpha_{k2}u_2+\cdots+\alpha_{kn}u_n,\ k=1,2,\cdots,$$

这里一切系数 α_i 和 α_{ki} 都是有理数. 因为 F 的每一个元素都可以写成 αa 的形状, 其中 $a\in G$, α 是有理数, 所以这个元素乘上某一数 p 的幂(例如, 等于在数 α 的分母中出现的每一个数 p 的幂), 就把它变成子群 G_p 的一个元素. 设 m 是这一个数, 它使得 $p^m u_1$, $p^m u_2, \cdots, p^m u_n$ 属于 G_p. 由元素 $x_1, x_2, \cdots, x_k, \cdots$ 的序列收敛于元素 x 推出, 数 $\alpha_{1i}, \alpha_{2i}, \cdots, \alpha_{ki}\cdots$ p 进收敛于数 α_i, $i=1,2,\cdots,n$. 于是根据 XI, 存在这样一个正整数 s, 使得

$$\alpha_i-\alpha_{si}\in p^m\mathfrak{J},\ i=1,2,\cdots,n.$$

因为 $\alpha_i-\alpha_{si}$ 是有理数, 所以根据 IV 得

$$\alpha_i-\alpha_{si}\in p^m\mathfrak{R}^{(p)},$$

因此

$$(\alpha_i-\alpha_{si})u_i\in G_p.$$

于是

$$x-x_s=\sum_{i=1}^{n}(\alpha_i-\alpha_{si})u_i\in G_p,$$

又因为 $x_s\in G_p$, 所以 $x\in G_p$.

我们暂时撇开群 P 与原来的群 G 的联系, 即只把 P 看成域 $\mathfrak{P}$ 上一个 n 维向量空间, 证明以下定理:

群 P 的每一个含有 $\mathfrak{P}$ 上 n 个线性无关元素的闭子群 H 都可以分解成直和

$$H=\mathfrak{P}v_1+\cdots+\mathfrak{P}v_k+\mathfrak{J}v_{k+1}+\cdots+\mathfrak{J}v_n,$$

其中数 k, $0\leqslant k\leqslant n$, 只依赖于群 H 本身.

首先假设子群 H 不含 $\mathfrak{P}$ 上任何非零子空间. 设 $u_1, u_2, \cdots, u_n$ 是 H 中任意一组在 $\mathfrak{P}$ 上线性无关的元素. 记

$$H_0=\mathfrak{J}u_1+\mathfrak{J}u_2+\cdots+\mathfrak{J}u_n;$$

换一句话说，H_0 是群 P 的含有元素 $u_1, u_2, \cdots, u_n$ 并且容许 p 进整数作乘法的最小子群. 注意 $H_0\subseteq H$. 事实上，对于任意有理整数 k 和 H 的任意元素 x，元素 kx 属于 H，而由 VI，任意 p 进整数都是有理整数序列的 p 进极限，又因为子群 H 是闭的，所以元素 x 与任意 p 进整数的乘积也属于 H.

现在令 H'_m 表示由群 P 的一切这样的元素所组成的子群，这些元素的 p^m 倍属于 H_0. 又令

$$H_m=H'_m\cap H, m=0,1,2,\cdots.$$

于是 $H_0\subseteq H_1\subseteq\cdots\subseteq H_m\subseteq\cdots$，并且这个递增序列的并集与 H 重合. 事实上，P 的任意元素可以写成元素 $u_1, u_2, \cdots, u_n$ 的以 p 进数为系数的线性组合，然而根据 XII，任意 p 进数都可以乘上数 p 的某一个幂使成为 p 进整数。

假设可以选出无限序列

$$H_0\subset H_{m_1}\subset H_{m_2}\subset\cdots\subset H_{m_t}\subset\cdots,$$

其中每一个子群 H_{m_t} 不等于 $H_{m_{t-1}}$. 于是在 H_0 里可以找到这样的元素序列 $x_1, x_2, \cdots, x_t, \cdots$，使得 $p^{-m_t}x_t$ 属于 H_{m_t}，但不属于 $H_{m_{t-1}}$. 因为由 IX，子群 H_0 是紧的，所以在这个序列里可以选出一个子序列，它收敛于 H_0 的某一元素 x. 于是根据 XI，对于任意 s，$s=1, 2, \cdots$，可以找到这样一个元素 $x_{t(s)}$，其中 $t(s)>s$，并且

$$x-x_{t(s)}\in p^sH_0.$$

因为用 p^{-s} 去乘空间 P 的元素是有意义的，由此得

$$p^{-s}x-p^{-s}x_{t(s)}\in H_0. \tag{2}$$

由于 $p^{-m_{t(s)}}x_{t(s)}\notin H_{m_{t(s)-1}}$，而 $1\leqslant s<t(s)\leqslant m_{t(s)}$，所以 $p^{-s}x_{t(s)}\notin H_0$，由(2)得 $x\neq 0$. 又因为 $p^{-s}x_{t(s)}\in H$，再由(2)得 $p^{-s}x\in H$. 这个结论对于所有的 s 都成立，又因为前面已经证明了 H 的元素与任意 p 进整数的乘积仍属于 H，所以 H 含有子群 $\mathfrak{P}x$，这个子群不等

于零，并且容许用 $\mathfrak{P}$ 的数作乘法，这与对于子群 H 所作的假设相违.

这就证明了存在这样的 m，使得

$$H_m = H_{m+1} = \cdots = H,$$

由此得 $H_0 \subseteq H \subseteq H'_m$. 根据 H_0 的构造，它是环 $\mathfrak{J}$ 上一个秩为 n 的自由模. 这对于 H'_m 也是对的——可以取 $p^{-m}u_1, p^{-m}u_2, \cdots, p^{-m}u_n$ 作为基. 于是，根据 X，可以把 § 22a 的结果应用到算子环 $\mathfrak{J}$ 上. 我们得出，子群 H 也是环 $\mathfrak{J}$ 上一个秩为 n 的自由模，即

$$H = \mathfrak{J}v_1 + \mathfrak{J}v_2 + \cdots + \mathfrak{J}v_n.$$

在这一情形，$k=0$.

如果 H 包含 $\mathfrak{P}$ 上非零子空间，那末令 K 是这些子空间的和. 因为 P 作为域上向量空间，是完全可约的——域的加法群作为这个域上带算子的群是单的——所以根据 § 61，子群 K 是 P 的一个直被加项，$P = K + L$，而

$$K = \mathfrak{P}v_1 + \mathfrak{P}v_2 + \cdots + \mathfrak{P}v_k,\ k \leqslant n.$$

另一方面，子群 L 是 $\mathfrak{P}$ 上 $n-k$ 维向量空间. 交 $D = H \cap L$ 也含有 $n-k$ 个在 $\mathfrak{P}$ 上线性无关的元素，但已不含关于 $\mathfrak{P}$ 的容许子群. 并且由于 H 是闭的，从而 D 也在 L 内是闭的. 于是我们就回到前面所考虑的情形，即

$$D = \mathfrak{J}v_{k+1} + \cdots + \mathfrak{J}v_n.$$

最后，根据 § 17，VII′，$H = K + D$. 定理完全被证明.

同时我们还看到，数 k 是 H 中关于 $\mathfrak{P}$ 的极大容许子群(在 $\mathfrak{P}$ 上)的秩，即这个数由群 H 本身所确定.

这个定理可以应用到群 $\overline{G}_p$ 上. 对于这一情形，由定理所得到的数 k，归根到底是由原来的群 G 唯一确定的，即是这个群的一个不变量. 我们把这个数叫做群 G 的 p-秩，并且用 k_p 来表示，$0 \leqslant k_p \leqslant n$. 其次，根据上面的定理，在子群 $\overline{G}_p$ 中所选取的任意一

组元素

$$v_1, \cdots, v_{k_p}, v_{k_p+1}, \cdots, v_n \tag{3}$$

都在 $\mathfrak{P}$ 上线性无关，因而是群 P 中元素(在 $\mathfrak{P}$ 上)的一个极大线性无关组. 另一方面，群 F 的任意一个(在 $\mathfrak{R}$ 上)极大线性无关元素组

$$u_1, u_2, \cdots, u_n \tag{4}$$

在群 P 内也是一个(在 $\mathfrak{P}$ 上)极大线性无关组. 由此推出，(3)和(4)中每一组的元素都可以由另一组元素(在 $\mathfrak{P}$ 上)线性表示；因此

$$u_i = \sum_{j=1}^{n} \alpha_{ij} v_j, \ i = 1, 2, \cdots, n,$$

这里所有的系数 α_{ij} 都是 p 进数，并且行列式 $|\alpha_{ij}| \neq 0$.

这样，对于群 G，有一个元素是 p 进数的 n 阶非退化方阵 $A_p = (\alpha_{ij})$ 与它对应. 然而方阵 A_p 依赖于组(3)和(4)的选取，所以我们应该弄清楚，当这两个组改变时，矩阵 A_p 如何改变.

设组(3)和(4)分别变成

$$v'_1, \cdots, v'_{k_p}, v'_{k_p+1}, \cdots, v'_n \tag{3'}$$

和

$$u'_1, u'_2, \cdots, u'_n, \tag{4'}$$

并且元素 $v'_1, \cdots, v'_{k_p}$ 在子群 $\overline{G}_p$ 里与组(3)的元素 $v_1, \cdots, v_{k_p}$ 扮演着同样的角色. 组(4)和(4′)是群 F 的两个极大线性无关组，因而它们在域 $\mathfrak{R}$ 上可以相互线性表示. 设(4′)通过矩阵 B 由(4)表示：

$$(u') = B(u)^{1)}.$$

B 是一个有理系数的 n 阶非退化方阵，并且每一个这样的方阵都把组(4)变成某一个组(4′).

与此相应，我们有

1) (u) 和 (u') 是组(4)与(4′)排成纵列的简写。

$$(v)=C_p(v').$$

方阵 C_p 给出群

$$\bar{G}_p=\mathfrak{P}v'_1+\cdots+\mathfrak{P}v'_{k_p}+\mathfrak{S}v'_{k_p+1}+\cdots+\mathfrak{S}v'_n$$

的一个自同构. 在这个自同构之下，子群 $K=\mathfrak{P}v'_1+\cdots+\mathfrak{P}v'_{k_p}$ 被映成自身. 因此 C_p 有形状

$$C_p=\begin{pmatrix} U & O \\ W & V \end{pmatrix}, \tag{5}$$

这里 U 是一个元素为 p 进数的 k_p 阶非退化方阵，V 是一个元素为 p 进整数的 $n-k_p$ 阶方阵，并且在环 $\mathfrak{S}$ 上有逆方阵，而 W 是一个元素为 p 进数的矩阵. 反之，任何形如(5)的方阵都给出群 $\bar{G}_p$ 的一个自同构，即使得组(3)变成某一个组(3′). 所有形如(5)的方阵对于乘法作成一个群. 我们把这个群记作 $\Gamma_p(n, k_p)$.

现在可以给出组(4′)通过组(3′)来表示的方阵 A'_p 了. 事实上，由 $(u)=A_p(v)$ 得

$$(u')=BA_pC_p(v'),$$

即 $A'_p=BA_pC_p$.

固定一个素数 p，方阵 A_p 与群 G 对应. 现在设对于一切素数，而且在取群 F 中同一个线性无关组(4)时都这样做了. 这样一来，如果 $p_1, p_2, \cdots, p_i, \cdots$ 是一切素数所成的序列，那么就有一个方阵序列

$$\mathfrak{A}=(A_{p_1}, A_{p_2}, \cdots, A_{p_i}, \cdots) \tag{6}$$

与群 G 对应，这里 A_{p_i} 是元素为 p_i 进数的一个 n 阶非退化方阵[1]. 序列(6)与序列

$$\mathfrak{A}'=(A'_{p_1}, A'_{p_2}, \cdots, A'_{p_i}, \cdots) \tag{7}$$

说是等价的，如果存在一个元素是有理数的 n 阶非退化方阵 B 和

1) 以下说到方阵序列总是指形如(6)的序列。

分别属于群 $\Gamma_{p_i}(n, k_{p_i})$ 的矩阵 C_{p_i}，使得对于每一个 i，都有等式

$$A'_{p_i}=BA_{p_i}C_{p_i}.$$

这个等价性显然是自反的，对称的和传递的，因而从以上的证明得出，序列(7)与群 G 对应，必要且只要它与(6)等价. 这样，群 G 唯一地确定方阵序列的一个等价类. 我们约定把这个类简记作 $(\mathfrak{A})_G$.

下面的定理是整个这一节的主要结果：

秩 n，对于一切素数 p 来说的 p-秩 k_p 以及方阵序列类 $(\mathfrak{A})_G$ 构成群 G 的一个完全不变量系.

设群 G 与 G' 具有同一秩 n，对于每一个素数 p，具有同一 p 秩 k_p，并且 $(\mathfrak{A})_G=(\mathfrak{A})_{G'}=(\mathfrak{A})$. 又设 F 和 F' 分别是包含 G 和 G' 的最小完备群，并且对于某一素数 p，令 P 和 P' 是 p 进数域上 n 维向量空间，它们分别是包含 F 和 F' 的最小向量空间. 在类 $(\mathfrak{A})$ 里选取一个序列 $\mathfrak{A}$，在这个序列里，对应于数 p 的矩阵是 A_p. 于是在 F 里存在这样一组线性无关的元素 $u_1, u_2, \cdots, u_n$，而对于群 G_p 的闭包，有这样一个直分解

$$\overline{G}_p=\mathfrak{B}v_1+\cdots+\mathfrak{B}v_{k_p}+\mathfrak{J}v_{k_p}+\cdots+\mathfrak{J}v_n,$$

使得组 $u_1, u_2, \cdots, u_n$ 通过矩阵 A_p 由组 $v_1, v_2, \cdots, v_n$ 来表示. 在群 F' 与 $\overline{G}'_p$ 里，相应地可以找到元素组 $u'_1, u'_2, \cdots, u'_n$ 和 $v'_1, v'_2, \cdots, v'_n$，使得第一组仍是通过矩阵 A_p 由第二组来表示.

对应 $u_1\to u'_1$, $u_2\to u'_2, \cdots$, $u_n\to u'_n$ 导致群 F 与 F' 的一个(在 $\mathfrak{R}$ 上)算子同构，这个同构唯一地开拓为群 P 与 P' 的一个(在 $\mathfrak{P}$ 上)算子同构. 多亏由 $u_1, \cdots, u_n$ 到 $v_1\cdots$, v_n 的过渡矩阵同由 $u'_1, \cdots, u'_n$ 到 $v'_1, \cdots$, v'_n 的过渡矩阵是同一个，所以元素 v_i 在这个同构之下被映成元素 v'_i, $i=1, 2, \cdots$, n，即子群 $\overline{G}_p$ 被同构地映成子群 $\overline{G}'_p$. 由此推出，交 $F\cap\overline{G}_p$ 被同构地映成交 $F'\cap\overline{G}'_p$；换句话说，在所建立的群 F 与 F' 的同构映射之下，子群 G_p 与 G'_p 相互对应. 因为根

据方阵序列 $\mathfrak{U}$ 的定义,元素组 $u_1, \cdots, u_n$ 与 $u'_1, \cdots, u'_n$ 不依赖于数 p 的选取，所以上述事实对于一切 p 都成立. 这样，一切子群 G_p 的交被同构地映成一切子群 G'_p 的交,即 G 与 G' 同构.

§ 32B 前节结果的补充和应用

前一节所建立的关于有限秩无扭阿贝尔群的完全不变量系还不能认为已经完成了对这一类群的分类. 事实上，我们现在还没有证明,对于任意给定的一组不变量,可以找到一个群，使它具有所给的这组不变量. 这还是不能证明的，因为实际上对应于上述意义下所写出的群的矩阵序列还具有一些附加性质，这些性质在上一节里没有被提到[1]. 我们现在就来讨论这些性质.

与群 G 对应的矩阵序列 $\mathfrak{A}$ 依赖于群 F 内线性无关组 u_1, u_2, $\cdots, u_n$ 的选取. 这一组元素可以取自群 G 本身. 在这一情形，对于所有的 p,它们包含在 $\bar{G}_p$ 内,即每一个元素 u_i, $i=1,2,\cdots,n$,被元素 $v_1, \cdots, v_{k_p}, v_{k_p+1}, \cdots, v_n$ 线性表示，其中元素 $v_1, \cdots, v_{k_p}$ 的系数是 p 进数,而其余元素的系数是 p 进整数. 换句话说,这时矩阵 A_p(对于所有的 p)的后 $n-k_p$ 列的元素都是 p 进整数. 这样的矩阵叫做*典范的*[2].于是对于我们所选取的元素组 $u_1, \cdots, u_n$,组成序列 $\mathfrak{U}$ 的所有矩阵都是典范的. 然而序列 $\mathfrak{U}$ 的这个性质当过渡到与它等价的序列时不被保持. 容易看出,尽管一个典范矩阵 A_p 右乘以群 $\Gamma_p(n, k_p)$ 的一个矩阵 C_p，仍然得到一个典范矩阵，但是一个典范矩阵左乘以一个有理系数的非退化矩阵 B 时，一般说来已不再是典范矩阵. 然而应该注意到，在矩阵序列的等价性的定义里出现的矩阵 B 对于所有的 p 来说都是同一个. 同时在这个矩阵

1) 在 Derry[1] 里也没有提到矩阵序列的这个附加性质,恰恰是关于具有给定不变量的群的存在问题在那里没有被考虑。

2) 我们看到,典范矩阵的定义依赖于群 G 的 p-秩 k_p。

的元素的分母里，只出现有限个素数，这就是说，除掉有限个数外，对于所有的 p，矩阵 B 可以认为元素是 p 进整数的矩阵. 这时乘积 BA_p 仍是典范矩阵. 这样，我们得到以下结果：

在与群 G 对应的类 $(\mathfrak{U})_G$ 的每一个矩阵序列 $\mathfrak{U}$ 里，所有的矩阵，除去有限个外，都是典范矩阵.

我们把由具有这个定理所指出的性质的矩阵序列所组成的类 $(\mathfrak{U})$ 叫做*典范类*，显然，远不是所有的类都是典范类.

引理 *每一个典范类 $(\mathfrak{U})$ 至少含有一个完全由典范矩阵所组成的序列.*

事实上，设 $\mathfrak{U}$ 是类 $(\mathfrak{U})$ 中任意一个序列，而 A_p 是这个序列里一个非典范的矩阵. 根据 XII，存在数 p 的这样一个幂 p^k，使得矩阵 A_p 通过左乘以一个纯量矩阵 p^kE 之后，后 $n-k_p$ 列的元素都变成 p 进整数，即矩阵 A_p 变成典范矩阵. 如果用 p^kE 从左边去乘序列 $\mathfrak{U}$ 的所有矩阵，我们就得到类 $(\mathfrak{U})$ 里一个序列，它里面的非典范矩阵要比 $\mathfrak{U}$ 里面的少：因矩阵 p^kE 去乘 $\mathfrak{U}$ 里面的每一个典范矩阵 $A_q, q\neq p$，并不破坏它的典范性. 应用上述方法有限次，我们就得到 $(\mathfrak{U})$ 里一个序列，它的所有矩阵都是典范的.

现在我们可以转来证明对于有限秩无扭阿贝尔群的完全描述的定理：

给定了一个自然数 n，对于每一素数 p，给定了一个满足条件 $0\leqslant k_p\leqslant n$ 的非负整数 k_p，以及与这些数相关联的矩阵序列的典范类 $(\mathfrak{U})$[1]，那末存在一个无扭阿贝尔群，它具有秩 n，p-秩 k_p，并且以类 $(\mathfrak{U})$ 作为与它对应的矩阵序列类.

为了证明，根据引理，在类 $(\mathfrak{U})$ 里可以选取一个完全由典范矩阵组成的序列 $\mathfrak{U}$. 再取一个秩为 n 的完备群 F，

1) 回忆在典范类 (u) 的定义里要用到数 n 和数 k_p.

$$F=\Re u_1+\Re u_2+\cdots+\Re u_n.$$

然后固定一个素数 p，并且将 F 嵌入 p 进数域 $\mathfrak{P}$ 上一个 n 维向量空间 P，

$$P=\mathfrak{P}u_1+\mathfrak{P}u_2+\cdots+\mathfrak{P}u_n.$$

在空间 P 里选取元素组 $v_1,\cdots,v_{k_p},v_{k_p+1},\cdots,v_n$，它通过序列 $\mathfrak{U}$ 的矩阵 A_p 的逆矩阵，由 $u_1\cdots,u_n$ 表示．令

$$V_p=\mathfrak{P}v_1+\cdots+\mathfrak{P}v_{k_p}+\mathfrak{J}v_{k_p+1}+\cdots+\mathfrak{J}v_n$$

再令 $D_p=F\cap V_p$，并且把所有子群 D_p 的交（p 遍历一切素数）记作 G.

群 G 就是所求的．

事实上，由矩阵 A_p 的典范性可知，元素 $u_1,\cdots,u_n$ 属于子群 V_p，从而属于 D_p．又根据序列 $\mathfrak{U}$ 的取法，这一个事实对一切 p 都成立．所以元素 $u_1,\cdots,u_n$ 属于子群 G．这就证明了，群 G 具有秩 n，从而 $F=\Re G$.

子群 V_p 是子群 D_p 在 P 内的闭包．事实上，元素组 $v_1,\cdots,v_n$ 是 P 中（在 $\mathfrak{P}$ 上）一个极大线性无关组，即

$$P=\mathfrak{P}v_1+\cdots+\mathfrak{P}v_n.$$

由于 $\mathfrak{J}$ 在 $\mathfrak{P}$ 内是闭的，子群 V_p 在 P 内是闭的，从而含有子群 D_p 的闭包 $\bar{D}_p$．另一方面，如果 x 是 V_p 的任意元素，那末因为子群 F 的闭包等于 P[1]，所以在 F 内存在元素序列 $x_1,x_2,\cdots,x_k,\cdots$，收敛于 x．根据 XI，存在一个数 m，使得当 $k>m$ 时，

$$x-x_k\in V_p,$$

从而 $x_k\in V_p$，即 $x_k\in D_p$．这就证明了，子群 $\bar{D}_p$ 与 V_p 重合．

为了完成定理的证明，只剩下证明，对于一切 p，等式 $\Re^{(p)}G=D_p$ 成立．

1）这个事实由 II 得出。

事实上，由 $\mathfrak{R}^{(p)}\subset\mathfrak{J}$ 得出，对于 $d\in D_p$, $\alpha\in\mathfrak{R}^{(p)}$，有 $\alpha d\in V_p$；又因为 $\alpha d\in F$，所以 $\alpha d\in D_p$，即 $\mathfrak{R}^{(p)}D_p=D_p$. 因此对于一切素数 p，都有 $\mathfrak{R}^{(p)}G\subseteq D_p$. 另一方面，设 x 是 D_p 的任意一个元素. 存在 G 的一个元素 a 和一个正整数 m，使得 $x=\frac{1}{m}a$. 如果 $m=p^{\alpha}m'$, $(m',p)=1$，那末当 $\alpha=0$ 时，将有 $\frac{1}{m}\in\mathfrak{R}^{(p)}$，即 $x\in\mathfrak{R}^{(p)}G$. 如果 $\alpha>0$，那末考虑元素

$$y=m'x=\frac{1}{p^{\alpha}}a.$$

对于一切异于 p 的素数 q, $\frac{1}{p^{\alpha}}\in\mathfrak{R}^{(q)}$，从而元素 y 属于 D_q. 元素 $y=m'x$ 同时也属于 D_p，即 $y\in G$. 因为 $\frac{1}{m'}\in\mathfrak{R}^{(q)}$，所以

$$x=\frac{1}{m'}y\in\mathfrak{R}^{(p)}G,$$

即 $\mathfrak{R}^{(p)}G=D_p$.

我们来指出所得到的关于有限秩无扭阿贝尔群的分类的一些应用. 我们知道，直和的秩等于直被加项的秩的和. 利用 p-秩的定义容易证明，上面这个事实对于 p-秩来说也成立. 其次，如果我们考虑秩为 1 的群 G，那末它的 p-秩等于零或 1. 在 § 30 里已经知道，这个群可以由等价的特征

$$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n,\cdots)$$

所组成的特征类给出，这里每一个 $\alpha_i=\alpha(p_i)$ 或者是零，或者是一个正整数，或者是符号 ∞，并且对应于 $\alpha(p_i)=\infty$ 的那些素数 p_i 不依赖于特征 α 在这个类里的选取. 当且仅当 $\alpha(p)=\infty$ 时，对于这样的 p，群 G 才有 p-秩 1. 事实上，令 $\mathfrak{P}G=P$，这里 $\mathfrak{P}$ 是 p 进数域. 如果 $\alpha(p)=\infty$，即对于 G 的任意元素 a 和任意正整数 m 来说，方程 $p^m x=a$ 在 G 中有解，从而 $\mathfrak{R}_pG=G$，这里 $\mathfrak{R}_p$ 是 p 进分数

环．现在由 III 得出，子群 G 在群 P 内的闭包等于 P，从而 $k_p=1$．如果 $\alpha(p)\neq\infty$，那末在 G 里可以取到这样的元素 a，使得与它对应的特征 α 有 $\alpha(p)=0$．这时根据 IV，

$$D\subseteq\mathfrak{R}^{(p)}a\subset\mathfrak{J}a,$$

从而 $k_p=0$[1]．

从上一段所作的说明可知，给定了秩，同时对于一切 p，给定了 p-秩，总可以作为适当选取的秩为 1 的群的直和，而构造出一个具有所给的秩和 p-秩的无扭群．是不是所有的有限秩无扭阿贝尔群都是秩为 1 的群的直和？如果这个问题的答案是肯定的，那末上面所给出的分类里面有很多情况将失去意义．然而实际上，正如同下面更为一般的关于不能分解成子群直和的群的存在问题的定理所指出的那样，这个问题没有肯定的答案（参看 Levi[1]，Понтрягин[1]，Курош[6]；也参看 § 32）：

对于任意正整数 n，存在秩为 n 的无扭阿贝尔群，它不能分解成直和．

证 设一个秩为 n 的无扭阿贝尔群 G 对某一素数 p 来说，有 p-秩 $n-1$，又设给出了 G 的一个直和分解 $G=G_1+G_2$，这里的被加项分别有秩 n_1 和 n_2，$n_1+n_2=n$．那末其中一个被加项，比如说，G_1 的 p-秩等于它的秩 n_1，而被加项 G_2 的 p-秩等于 n_2-1．在前一节里，用以作出关于群 G 的矩阵 A_p 的元素组(3)和(4)现在可以把关于群 G_1 和 G_2 的相应的元素组拼接起来而得到．这时矩阵 A_p 有形状

$$A_p=\begin{pmatrix}M & 0\\ 0 & N\end{pmatrix},$$

1) 用我们所建立的关于任意有限秩的群的不变量的语言对 § 30 所给出的秩为 1 的群完全分类，留给读者去完成。

这里M和N分别是n_1阶和n_2阶方阵. 我们可以认为矩阵A_p是典范的,即矩阵N的最后一列是由p进整数所组成. 我们知道,在另外选取元素组(3)和(4)时与G相对应的矩阵A'_p有形状$A'_p=BA_pC_p$, 这里B是一个元素是有理数的n阶非退化矩阵, 而C_p是群$\Gamma_p(n,n-1)$里的一个矩阵. 矩阵C_p的最后一列里, 除最后一个元素是一个不等于零的p进整数外,其它所有元素都等于零. 因此,矩阵A_pC_p有形状

$$A_pC_p=\left(S\,\middle|\,\frac{0}{T}\right),$$

这里S是一个有n行,$n-1$列的以p进数为元素的矩阵, 而T是一个有n_2行一列的以p进整数为元素的矩阵. 其次,如果令B'表示由B的后n_2列所构成的矩阵,那末矩阵BA_pC_p的最后一列等于乘积$B'T$. 因此, 这一列的元素是关于T的元素的有理系数的线性型,因为$n_2<n$,所以在有理数域$\mathfrak{R}$上线性相关.

域$\mathfrak{R}$是可数的,由VIII, 环$\mathfrak{J}$有连续统的势. 因此可以作出这样一个p进元素的n阶非退化矩阵A_p,它的最后一列由在有理数域$\mathfrak{R}$上线性相关的p进整数所组成. 令$k_p=n-1$,并且对于一切$q\neq p$,随意给定q-秩$k_q(0\leqslant k_q\leqslant n)$,和相应的典范矩阵$A_q$,如同本节中所证明的那样,定义一个秩为$n$的无扭阿贝尔群$G$,那末由上一段所作的说明可知,这个群不能分解成直和.

名 词 索 引

节号

三 画

四 画

五 画

六 画

七 画

八 画

九 画

十 画

十 一 画

十 二 画

十 三 画

十 四 画

十 五 画

其 它

[G e n e r a l   I n f o r m a t i o n]
书名= 群论　上册
作者= （苏）A . г . 库洛什
页数= 2 7 7
S S 号= 1 0 1 7 9 7 9 1
出版日期= 1 9 8 7 年0 7 月第1 版